VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZAVEDENÍ MANAGEMENTU BEZPEČNOSTI INFORMACÍ V PODNIKU DLE ISO 27001

IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT IN COMPANY ACCORDING TO ISO 27001

DIPLOMOVÁ PRÁCE
MASTER‘S THESIS

AUTOR PRÁCE
AUTHOR

Bc. ADAM ŠUMBERA

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. PETR SEDLÁK

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Šumbera Adam, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Zavedení managementu bezpečnosti informací v podniku dle ISO 27001

v anglickém jazyce:

Implementation of Information Security Management in Company According to ISO 27001

Pokyny pro vypracování:

Osnova zadání:
Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky. Praha: Český normalizační institut, 2006.
ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů. Praha: Český normalizační institut, 2008.
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.
SMEJKAL, V. a K. RAIS Řízení rizik ve firmách a jiných organizacích. Praha: Grada Publishing, 2010. ISBN 978-80-247-3051-6.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 15.05.2013

Abstrakt

Diplomová práce se zabývá tématem zavádění systému řízení bezpečnosti informací v podniku. Teoretická část práce shrnuje teoretické poznatky z oblasti bezpečnosti informací a popisuje sadu norem ČSN ISO/IEC 27000. V další části je provedena analýza společnosti, na kterou jsou poté v praktické části práce aplikovány teoretické poznatky při zavádění systému bezpečnosti informací.

Abstract

This diploma thesis deals with implementation of the information security management system in company. The theoretical part of thesis summarizes the theoretical knowledge in the field of information security and describes a set of standards ISO/IEC 27000. In the following section the specific company is analysed, and to this company there are then applied theoretical knowledge during the implementation of information security management system.

Klíčová slova

Řízení bezpečnosti informací, ISMS, analýza rizik, PDCA cyklus, ISO/IEC 27000, aktivum, hrozba, zranitelnost, riziko, opatření, příručka bezpečnosti.

Keywords

Information security management system, ISMS, risk analysis, PDCA cycle, ISO/IEC 27000, asset, threat, vulnerability, risk, countermeasure, security manual.

Bibliografická citace

ŠUMBERA, A. Zavedení managementu bezpečnosti informací v podniku dle ISO 27001. Brno: Vysoké učení Technické v Brně, Fakulta podnikatelská, 2013. 89 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že jsem celou diplomovou práci zpracoval samostatně, na základě uvedené literatury a pod vedením svého vedoucího diplomové práce. Prohlašují, že citace použitých pramenů je úplná, a že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb. O právu autorském a o právech související s právem autorským).

V Brně dne 20.5.2013

……

Poděkování

Chtěl bych poděkovat především vedoucímu mé diplomové práce, panu Ing. Petru Sedlákovi za praktické rady a připomínky, které mi pomohly při tvorbě této práce. Děkuji také své rodině a blízkému okolí za podporu.

Obsah

Seznam použitých zkratek

Informační systém **(IS)**.

Informační a komunikační technologie (**ICT)**.

Mezinárodní organizace pro standardizaci **(ISO)**.

Mezinárodní úřad pro elektrotechniku **(IEC)**.

Česká technická norma **(ČSN)**.

British Standard **(BS)**.

Systém řízení bezpečnosti informací **(ISMS)**.

Demingův cyklus (Plánuj, dělej, kontroluj, jednej) **(PDCA)**.

komunikační standard pro bezdrátový přenos dat Wireless Fidelity **(Wi–Fi)**.

Licence opravňující využití prostředků serveru na straně klienta **(CAL)**.

Nepřerušitelný zdroj napájení **(UPS)**.

Pult centralizované ochrany **(PCO)**.

Technika útoku na internetové služby způsobující jejich ochromení **(DoS)**.

Distribuovaný DoS útok **(DDos)**.

Telefonní připojení využitelné pro vysokorychlostní přenos dat **(ADSL)**.

Datové úložiště obsahující pevné disky a rozhraní pro připojení k počítačové síti **(NAS)**.

Identifikace pomocí čipu vysílajícího rádiovou frekvenci **(RFID)**

(15)

1 Úvod

Nejcennějším majetkem společnosti jsou často informace. Ať už v podobě výrobní dokumentace, účetnictví, nebo třeba obchodních kontaktů a smluv. Proto je v dnešní době takřka nemyslitelné obejít se bez jejich ochrany, především proti jejich poškození, neoprávněnému užití, či odcizení. Značná část podniků si však plně neuvědomuje důležitost svých dat a možné důsledky toho, když by se strategické informace dostaly do nepovolaných rukou.

Informace jsou vystavovány hrozbám z různých směrů. Může jít o úmyslné incidenty, které jsou vedené lidskými subjekty, jako například počítačové podvody, sabotáže, vandalizmus, napadení počítačovými viry, útoky hackerů a útoky typu odepření služby, které jsou dnes stále častější. Může se jednat o hrozby neúmyslné, mezi které kromě jiných patří požáry, povodně, výpadky elektrických sítí, selhání hardwaru, softwarové chyby nebo selhání lidského faktoru, jako je častá neodborná manipulace a další.

Kromě ztráty je významným bezpečnostním problémem také průmyslová špionáž a konkurenční zpravodajství (Competitive intelligence).

Disciplína, která se zabývá ochranou citlivých dat v podniku, se nazývá management informační bezpečnosti (Information Security Management System), označuje se zkratkou ISMS a je popsána (mimo jiné) normou ISO/IEC 27001. Tento systém řízení bezpečnosti informací poskytuje model pro ustavení, implementaci, monitorování a zlepšování ochrany informačních aktiv tak, aby podporoval dosažení cílů organizace a minimalizoval obchodní ztráty.

ISMS zahrnuje celou řadu problémů a jejich řešení. Zabezpečení sítě, fyzických spojů a serveru, kódování datových přenosů, digitální podpisy, firemní směrnice, autentizace, autorizace, antivirovou a antispamovou ochranu, ochranu firemních aktiv, analýzu rizik, zálohování a další.

Menší firmy se často brání zavádění certifikovaných norem. Obávají se administrativních úkonů a výdajů spojených s certifikací. Certifikát ISO však není nutnou podmínkou pro zavedení řízení informační bezpečnosti. Implementaci jednotlivých doporučení si tak může firma upravit podle svých vlastních potřeb. Zejména podle rozsahu systému, počtu uživatelů, způsobu zpracování dat, jejich hodnoty, a především podle

reálných bezpečnostních rizik. Je běžné, že strategie ISMS není u malých podniků zpracována tak detailně jako u velkých firem.

U středně velkých firem je již organizace informační bezpečnosti nezbytná a je zde potřeba počítat s patřičnými finančními výdaji. V těchto firmách již existuje určitá míra anonymity mezi zaměstnanci a může zde snadno docházet k interním bezpečnostním incidentům. Jestliže nejsou přesně definována pravidla pro nakládání s informacemi a chování ve firemní síti, někteří zaměstnanci svým chováním úmyslně, či neúmyslně způsobují narušení bezpečnosti. Tato rizika jsou stejně závažná jako externí útoky a často hůře zjistitelná.

Informační a komunikační technologie jsou dnes nepostradatelnou složkou v každém oboru podnikání. Výpadek těchto služeb lze posuzovat jako finanční ztrátu, která se každou minutou zvyšuje a může vézt k úplnému ochromení společnosti. Je proto důležité zabývat se také tématy dostupnosti a integrity dat. (7) (10)

2 Vymezení problému a cíle práce

2.1 Vymezení problematiky

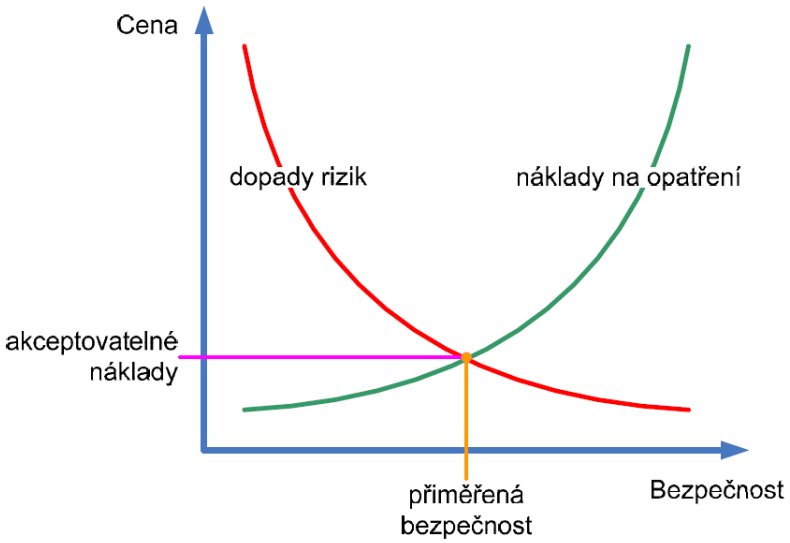
Problematika managementu informační bezpečnosti má tendenci se postupně uplatňovat i v menších soukromých podnicích, jak si jejich vedení začíná uvědomovat hodnotu vlastních dat, informací a celkové ICT infrastruktury podniku. Nejúčinnějším opatřením proti působícím vnějším, či vnitřním hrozbám, je nasazení jasných a přesných bezpečnostních standardů. To lze provést buď vytvořením struktury vlastních standardů, což přináší riziko opomenutí důležitého segmentu celkové bezpečnosti, nebo použít standardy již existující a ověřené. Nejrozšířenějším a celosvětově používaným standardem je ISO/IEC 27001 – Information Security Management Systems.

Předmětem této práce je analýza interního prostředí zvolené firmy za účelem nalezení bezpečnostních hrozeb pro firemní aktiva, jejíž součástí je také vypracování dotazníku, který bude mít za úkol prověřit povědomí zaměstnanců organizace o informační bezpečnosti. Dalším úkolem je provedení analýzy rizik a návrh podoby příručky bezpečnosti, tedy metodiky pro zavedení systému řízení bezpečnosti v podniku. Tato příručka slouží ke zdokumentování všech bezpečnostních opatření a k objasnění bezpečnostních principů uživatelům a manažerům.

O výsledky této práce se může v budoucnosti podnik dále opírat při případné certifikaci podnikového ISMS dle ISO/IEC 27001, bude-li časem tento certifikát vyžadován zákazníky. Proces certifikace ISMS by v této firmě neměl být problémem, jelikož v minulosti již absolvovala certifikaci ISO 9001 a obě normy jsou kompatibilní a certifikace probíhá obdobně.

2.2 Cíle práce

Cílem práce je pomocí systémového přístupu pro danou problematiku stanovit rovnováhu mezi přijatelným bezpečnostním rizikem, náklady na potřebná opatření a zátěží, kterou bezpečný systém působí na jednotlivé uživatele a správce. Hlavním cílem je důkladně analyzovat situaci ve firmě, identifikovat případná bezpečnostní rizika a v závislosti na reálných potřebách firmy stanovit podobu obecného předpisu pro tvorbu metodické příručky bezpečnosti.



Obrázek 1: Vztah mezi mírou rizika a náklady na opatření. Zdroj (8)

2.2.1 Příručka bezpečnosti informací

Je jedním z dokumentů potřebných pro úspěšné ustavení, provoz a budoucí zlepšování ISMS v podniku. Dokumentaci spojenou s bezpečností informací lze rozdělit na několik úrovní.

Na nejvyšší úrovni jsou dokumenty, které přímo vyžaduje systém řízení bezpečnosti informací, a jsou povinné pro úspěšnou certifikaci. Mezi ně patří definice rozsahu ISMS, politika ISMS, hodnocení a zvládání rizik apod.

Na druhé úrovni se nachází dokumentace sloužící k podpoře a prosazování ISMS, přizpůsobená potřebám konkrétní organizace. Tato dokumentace se souhrnně označuje jako

příručka bezpečnosti informací a definuje dílčí procesy a postupy, které zajišťují efektivní prosazení jednotlivých bezpečnostních opatření. Definuje kdo, co, kdy a jak má učinit, a objasňuje bezpečnostní principy všem uživatelům a manažerům.

Na nejnižší úrovni bezpečnostní dokumentace se nacházejí pracovní postupy popisující jednotlivé úkony. Tato úroveň však není nezbytná a lze ji řešit odkazem na dokumentaci příslušných použitých systémů. (7)

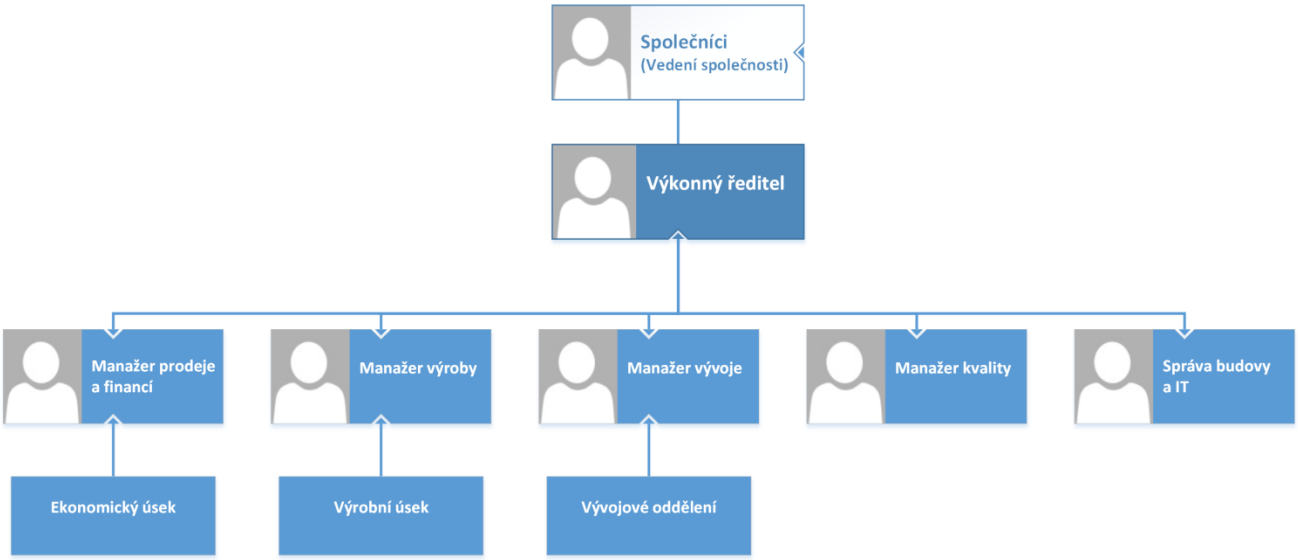
Struktura příručky bezpečnosti informací vychází z normy ISO/IEC 27001:2005 a má následující podobu:

1. Předmět normy
2. Normativní odkazy
3. Termíny a definice
4. Systém managementu bezpečnosti informací
5. Odpovědnost vedení
6. Interní audity ISMS
7. Přezkoumání ISMS vedením organizace
8. Zlepšování ISMS (1)

Návrhem konkrétní podoby této příručky pro analyzovanou společnost se zabývá kapitola 6.5.

3 Profil společnosti

Společnost, na kterou je zaměřena tato práce, je středně velkou firmou zabývající se vývojem, konstrukcí a výrobou elektroniky pro automobilový průmysl. Sídlí ve vlastní budově a zaměstnává 60 zaměstnanců. Z nich 45 pracuje ve výrobě a zbytek v administrativě a vývoji. Společnost působí jak na domácím, tak především na zahraničním trhu. Od roku 2006 je držitelem certifikátu kvality ČSN EN ISO 9001:2009. Vzhledem k závažnosti informací probíraných v této práci si nepřála být jmenována.



Obrázek 2: Organizační struktura společnosti. (Vytvořeno pro potřeby DP)

Povaha dat informací zpracovávaných a uchovávaných v podniku:

Jde o českého výrobce elektroniky, který z pochopitelných důvodů nemůže cenově ani objemem výroby konkurovat asijské produkci. Zaměřuje se tedy na vlastní vývoj. Ten je pro společnost klíčovým faktorem úspěchu. Pracuje se zde tedy převážně s daty, jako jsou návrhy elektrických schémat, zdrojové kódy programů pro mikrokontrolery, výrobní dokumentace k výrobkům, osobní údaje o zaměstnancích, obchodní smlouvy a softwarové licence.

4 Teoretická východiska

Hlavním cílem procesu ISMS je chránit aktiva společnosti (především informace) a zabránit jejich poškození, ztrátě nebo zneužití. Tento proces je popsán mimo jiné mezinárodními normami řady ISO 27000.

4.1 Důležité pojmy

Na **bezpečnost informací** lze nahlížet jako na celý soubor aktivit. Pomocí nich je nutné zajistit tyto hlavní pilíře bezpečnosti:
Důvěrnost – zajištění přístupu k informaci pouze autorizovaným jedincům a procesům.
Integrita – zajištění správnosti a úplnosti (neporušenosti) informací.
Dostupnost – zaručuje přístup k informacím oprávněným uživatelům v okamžiku, kdy je potřebují.

Kromě výše uvedených pojmů můžeme sledovat také další vlastnosti jako je například **autenticita**, **odpovědnost**, **nepopiratelnost** a **spolehlivost**.

Obrázek 3: Vztah mezi důvěrností, dostupností a integritou. (6)

Aktivum – hmotné i nehmotné statky, které mají pro vlastníka jistou hodnotu. Mezi hmotná aktiva se řadí například technické vybavení, prostředky výpočetní techniky, kabelové rozvody a ostatní zařízení. Mezi nehmotná pak především data a informace, software nebo služby (např. dodávka elektřiny, vody, topení atd.).

Bezpečnost – vlastnost nějakého systému, která vyjadřuje míru jeho odolnosti vůči možným hrozbám a škodám. Při návrhu a zavádění bezpečnosti informací je vhodné vzít v úvahu následující axiomy:

- Neexistuje absolutně bezpečný systém.
- Bezpečnost záleží především na lidech.
- Technologie jsou jen nástroje k prosazení bezpečnosti.
- Celková bezpečnost je určena nejslabším článkem v řetězci bezpečnostních opatření.
- Bezpečnost je dynamický proces, který podléhá neustálému vývoji a hodnocení.
- Bezpečnost komplikuje a znesnadňuje práci uživatele.
- Nelze slučovat funkce výkonné a kontrolní ve všech fázích životního cyklu systému.
- Uživatelům je vhodné přidělovat jen minimální pravomoci nezbytné pro jejich práci.
- Bezpečnost systému musí být zachována i po obnově provozu systému.

Hrozba – zneužití zranitelnosti. Jejím působením může dojít ke zničení, nebo ztrátě hodnoty aktiva. Jde o potenciální příčinu ohrožení bezpečnosti. Hrozby se rozdělují na **lidské** (ty mohou být úmyslné nebo neúmyslné), **technologické** a **přírodní**.

Zranitelnost – slabé místo systému, aktiva nebo opatření, které může být zneužito hrozbou a následně vést k poškození nebo znehodnocení aktiv, případně k neautorizovanému přístupu ke zdrojům systému.

Riziko – míra ohrožení konkrétního aktiva. Jde o kombinaci hrozby a zranitelnosti. Jejich společné působení může mít za následek vznik škody na daném aktivu – má na aktivum určitý dopad.

Dopad – nepříznivé účinky rizika na aktivum. Mohou to být buď bezprostřední finanční ztráty (např. zničení počítače, ztráta trhu apod.), nebo také účinky projevující se postupně (např. postupná ztráta dobrého jména firmy nebo pravidelný únik informací apod.). Dopady hrozeb je vhodné, pokud možno, převádět na finanční hodnoty. Ideální vyčíslení škody je v pořizovací ceně příslušného nového technického prostředku, nebo nákladů nutných vynaložit na obnovu provozu IS/ICT.

Opatření – umožňuje snížit sílu hrozby, která na systém působí, nebo úplně zabránit v jejím účinku. Jde o nástroj řízení rizika a může mít charakter **administrativní** (různé směrnice),

fyzický (fyzické zabezpečení, zámky, trezory), nebo **technický** (ochrana hesly a řízení přístupu pomocí autorizace a autentizace).

Data – pojmy data a informace se v praxi často zaměňují nebo slučují. Pro efektivní komunikaci je tedy vhodné tyto pojmy odlišit a vymezit jejich vzájemný vztah. Data jsou obvykle chápána jako statická fakta a jsou základním materiálem pro informace. Jde o vyjádření faktů a poznatků ve formě, která je vhodná pro další zpracování a přenos.

Informace – význam přisouzený datům. Jsou to sdělení (zpracovaná do podoby užitečné pro příjemce), z nichž se dovídáme něco nového, a tím dochází ke snižování dosavadní neurčitosti, o nějakém jevu nebo události. Každá informace je tedy datem, ale naopak neplatí, že jakákoliv data jsou zároveň informacemi. Těmi se stávají až v okamžiku, kdy příjemci přinesou nějaké poznání. (7) (10)

4.2 Normy v oblasti ISMS

Normy pro ISMS vycházejí z britského standardu z roku 1995, BS 7799, který se zabývá dostupností, důvěrnosti a integritou informací, případně celých podnikových informačních systémů. Je zaměřen na identifikaci hrozeb a tvorbu opatření pro snížení rizika.

V roce 2000 byl standard BS 7799 přijat jako mezinárodní norma pod názvem ISO 17799 a v roce 2005 byla vypracována sada norem řady ISO/IEC 27000. (7)

4.2.1 Sada norem řady ISO/IEC 27000

ČSN ISO/IEC 27000:2009

Zavádí pojmy, definice a terminologii pro všechny následující normy řady 27000. Vysvětluje principy ISMS založené na modelu PDCA a popisuje kritické faktory úspěchu implementace ISMS. Byla vydána v červnu 2009.

ČSN ISO/IEC 27001:2005

Podle ní se systémy řízení bezpečnosti informací certifikují. Tato norma poskytuje organizacím návod a požadavky na zavedení ISMS. Obsahuje soubor pravidel pro ochranu a bezpečnost informačních aktiv (tedy nejen informací, ale např. klíčového hardwaru, softwaru, zaměstnanců, know-how atd.) uvnitř organizace.

Normu tvoří devět kapitol a tři přílohy. První kapitola se zabývá procesním přístupem pro zavedení, provozování, udržování a zlepšování ISMS v organizaci. Popisuje čtyři fáze cyklu PDCA. Další tři kapitoly popisují předmět normy, přehled dokumentů, vymezení termínů a definic potřebných pro pochopení problematiky. Čtvrtá kapitola podrobně definuje požadavky jak na samotné ISMS, tak na tvorbu dokumentace a pořizování záznamů o průběhu procesů. Další kapitoly stanovují požadavky na vedení organizace, jako je zajištění zdrojů pro funkce ISMS, školení, zajištění informovanosti a odborné způsobilosti personálu, který vykonává práci související s ISMS. Zabývá se také požadavky pro interní audit a zlepšování systému.

Norma jasně popisuje jak postupovat a taxativně nařizuje, kterých cílů a bezpečnostních opatření musí být dosaženo. Tato část se nazývá Příloha A a je klíčovým dokumentem při zavádění ISMS.

Norma byla vydána v roce 2005 a nahrazuje normu ČSN BS 7799-2, která vychází z doporučení BS 7799 publikovaného Britským normalizačním institutem v roce 1995. Norma BS 7799 položila základy pro zavádění a implementaci managementu bezpečnosti informací ISMS.

ČSN ISO/IEC 27002:2005

Obsahuje sbírku nejlepších bezpečnostních praktik a seznam postupů, které jsou vhodné pro bezpečnost informací v organizaci provést. Je rozdělena na 11 oblastí obsahujících celkem 39 tzv. kategorií bezpečnosti a celkem obsahuje 133 opatření s doporučeními k jejich realizaci. Dále se norma v kapitole 4 zabývá informacemi o procesech hodnocení a zvládání rizik. Každá kategorie bezpečnosti obsahuje cíl, specifikující čeho má být dosaženo a související opatření, která je možné využít pro dosažení stanoveného cíle.

Hlavní oblasti normy ISO 27002 jsou:

- Bezpečnostní politika.
- Organizace bezpečnosti.
- Klasifikace a řízení aktiv.
- Bezpečnost lidských zdrojů.
- Fyzická bezpečnost a bezpečnost prostředí.
- Řízení komunikací a provozu.
- Řízení přístupu.
- Akvizice, vývoj a údržba IS.
- Zvládání bezpečnostních incidentů.
- Řízení kontinuity činností organizace.
- Soulad s požadavky.

Postupy zveřejněné v této normě mohou být využity jako základ pro tvorbu specifických směrnic na míru jakékoliv organizaci. Je možné použít pouze některá z těchto opatření, nebo naopak může být nutné zavést i další opatření, která v normě nejsou uvedena.

Norma téměř kompletně vychází ze svého předchůdce - normy ČSN ISO/IEC 17799, která má původ v první části britské normy BS 7799 z roku 1995.

ČSN ISO/IEC 27003:2010

Poskytuje implementační návody pro ostatní normy řady 27000.

Norma popisuje proces plánování ISMS (v souladu s požadavky normy ISO/IEC 27001) v pěti etapách: Získání souhlasu vedení se zahájením projektu; definování rozsahu a politiky ISMS; analýza požadavků bezpečnosti informací; ohodnocení a zvládání rizik; návrh ISMS.

Výstupem poslední etapy je tedy konkrétní finální plán implementace projektu ISMS organizace. V přílohách této normy je uveden kontrolní seznam činností potřebných k ustanovení a implementaci ISMS, popis rolí a odpovědností bezpečnosti informací, informace o interním auditování, struktury politik a informace o monitorování a měření bezpečnosti informací.

ČSN ISO/IEC 27004:2009

Tato norma poskytuje doporučení pro vývoj a používání metrik a pro měření účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a účinnosti opatření, podle ISO/IEC 27001. To zahrnuje procesy rozvoje metrik, samotné měření, analýzy dat a proces vyhodnocení a zlepšování programu měření bezpečnosti informací. V příloze normy jsou pak uvedeny příklady konceptů pro určitá opatření a procesy ISMS.

ČSN ISO/IEC 27005:2011

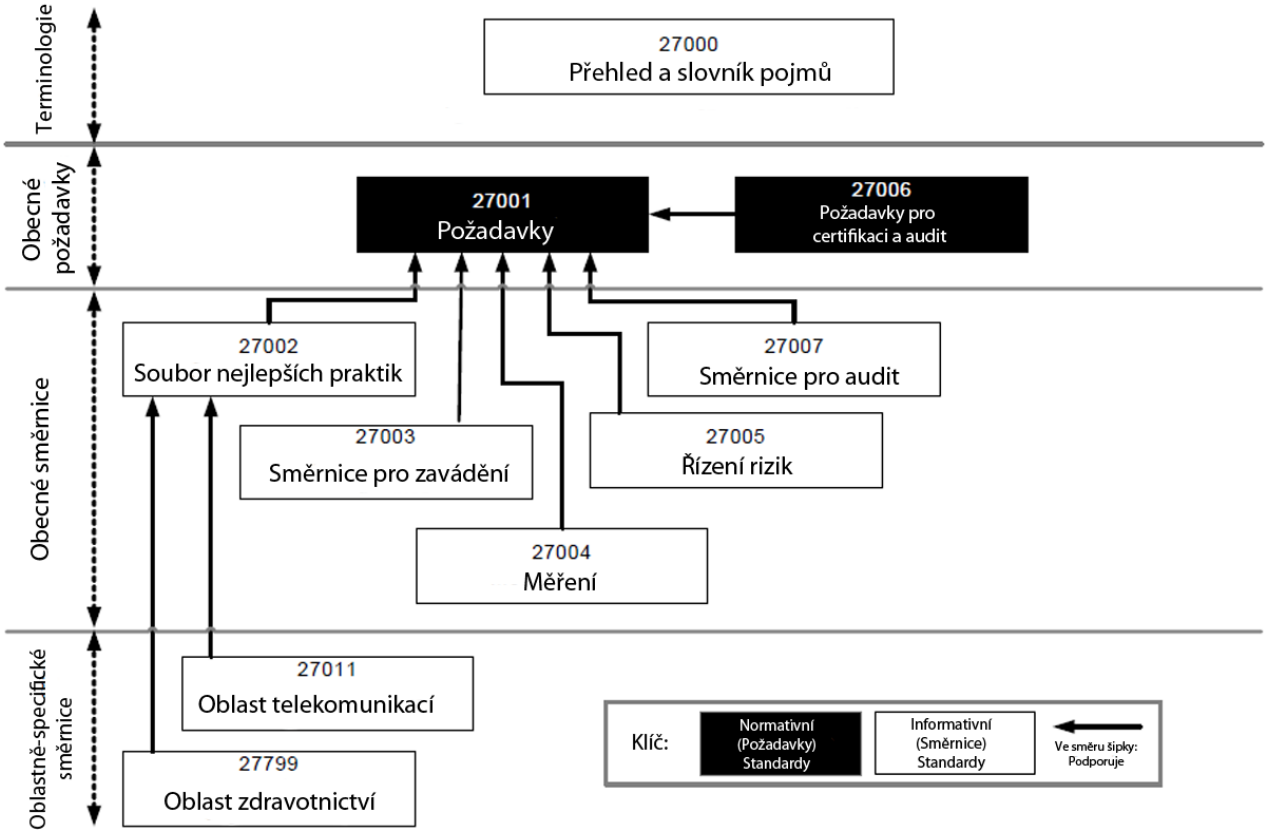
Norma se zaměřuje na řízení bezpečnostních rizik informačních technologií. Poskytuje doporučení pro řízení rizik v rámci organizace, podporuje obecný koncept specifikovaný v ISO 27001. Nenabízí však konkrétní metodiku pro řízení rizik bezpečnosti informací. Záleží na každé organizaci, jaký přístup vzhledem k rozsahu vlastního ISMS, stylu řízení rizik nebo povaze podnikání. V souladu s přístupem k řízení rizik popsaným v této normě lze pro implementaci požadavků ISMS použít některou z celé řady existujících metodik pro řízení rizik. Norma je určená manažerům a pracovníkům, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací a tam, kde je to relevantní, také externím subjektům.

Aktuální verze normy byla vydána v roce 2011 a navazuje na starší normy jako je ISO/IEC TR 13335 a BS 7799.

ČSN ISO/IEC 27006:2007

Stanovuje požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací. Vychází z normy ISO/IEC 17021, která nastavuje kritéria pro organizace zabývající se auditem případně certifikací systému řízení organizace a tyto kritéria dále doplňuje s četnými odkazy na normu ISO 27001. Klade požadavky na odbornou způsobilost a spolehlivost orgánů poskytujících certifikace ISMS.

Text této normy je rozdělen do deseti kapitol a doplněn čtyřmi přílohami. Cílem této normy je také poskytnout certifikačním autoritám kritéria, vůči kterým mají provádět audity ISMS, a nastínit časové nároky na úspěšné auditování. (7)



Obrázek 4: Grafický přehled vztahů v rodině norem řady ISO 27000. Upraveno pro potřeby DP podle (1)

4.2.2 Další standardy a legislativa v oblasti bezpečnosti ICT

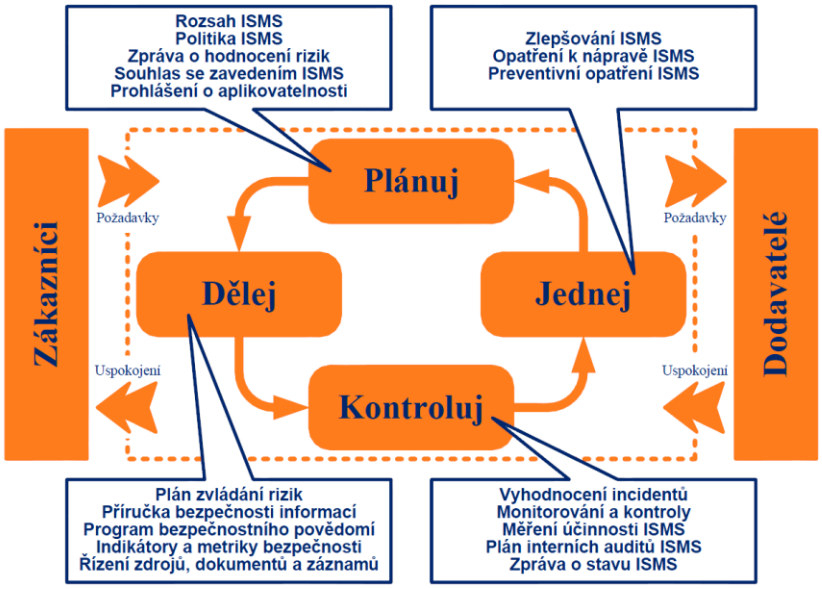
Kromě norem rodiny ISO/IEC 27000 se pro dosažení potřebného stupně zabezpečení důležitých dat využívají i další obecně přijímané standardy a metodiky. Mezi nejznámější patří knihovna ITIL a struktura COBIT. Zavádění bezpečnosti informací je možno opřít i o mezinárodní standard označovaný jako Common Criteria a v neposlední řadě o normu ISO/IEC 20000 popisující management kvality služeb v oblasti IT. Podrobnější popis těchto standardů by však výrazně přesahoval rámec této práce.

Na tomto místě uvádím i několik právních norem, které s oblastí řízení bezpečnosti informací v podniku souvisí. Jde především o tyto zákony:

- zákon č. 101/2000 Sb., o ochraně osobních údajů;
- zákon č. 148/1998 Sb., o ochraně utajovaných skutečností (v roce 2002 novelizován a částečně nahrazen jinými zákony);
- zákon č. 227/2000 Sb., o elektronickém podpisu;
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy;
- zákon č. 480/2004 Sb., o některých službách informační společnosti;
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

4.3 Cyklus PDCA

Podstatou celého procesu nazývaného ISMS, je takzvaný PDCA cyklus, známý také pod označením Demingův model. Z Obrázek 5 je patrné, že se jedná o nikdy nekončící proces, který zavádí kontinuální systém řízení bezpečnosti informací v organizaci. Jeho jednotlivé kroky, tedy Plánuj (**P**lan), Dělej (**D**o), Kontroluj (**C**heck) a Jednej (**A**ct) zaručují, že zavedení systému nebude jen jednorázovou aktivitou, ale neustálým koloběhem. (7)



Obrázek 5: Cyklus PDCA. (9)

Tento model zlepšování procesů je založen na postupu, který zavedl W. Edwards Deming, americký průkopník na poli managementu, který se proslavil po II. světové válce svojí činností v Japonsku, které pomohl hospodářsky postavit na nohy. Zavedl postup kontinuálního zlepšování, jehož součástí je právě PDCA model, který byl převzat do mnoha odvětví. (13)

Model ISMS využívá pro svůj životní cyklus právě tyto 4 etapy. **Ustanovení ISMS** – cílem je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření. **Zavádění a provoz ISMS** – cílem je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace. **Monitorování a přezkoumání ISMS** – cílem je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací. **Údržba a zlepšování ISMS** – cílem je realizace možností zlepšování systému řízení bezpečnosti informací, ať už soustavným zlepšování systému, nebo odstraňování zjištěných slabin a nedostatků. (9)

4.4 Přínosy ISMS

Zavedený proces managementu informační bezpečnosti přináší společnosti řadu výhod a přidaných hodnot. V této kapitole bych je rád shrnul a vyzdvihnul ty nejpodstatnější.

Jedním z důležitých přínosů pro společnost je inventura vlastních, nejen informačních, aktiv a uvědomění si jejich skutečných hodnot na základě vyčíslených škod souvisejících s jejich poškozením či ztrátou. Zavádí přechod od nesystémového a neuceleného řízení bezpečnosti k řešení komplexnímu.

Proces ISMS podporuje soustavné zvyšování bezpečnostního povědomí zaměstnanců a využívá jasně definovaných rolí, povinností a odpovědností. Přispívá tak k optimalizaci firemních procesů.

Důležitý je taktéž soulad s legislativou, především se zákonem č. 101/2000Sb o ochraně osobních údajů a snížení rizik souvisejících s únikem či ztrátou osobních dat o zaměstnancích. Společnost je díky tomu na veřejnosti lépe vnímána a působí důvěryhodněji i pro obchodní partnery. To podniku nepopiratelně přináší konkurenční výhodu.

Systém ISMS omezuje přístup nepovolaných osob do vymezených prostor. Eliminuje možnost krádeží či úmyslného poškození vybavení společnosti. Zavedení systému je ekonomicky efektivní. Náklady se vrátí zejména cestou minimalizace ekonomických ztrát, plynoucích z částečné nebo úplné ztráty, z vyzrazení informací či z výpadku procesů společnosti.

Systém bezpečnosti informací definuje i postupy při přijímání nových zaměstnanců a procesy při ukončení pracovního procesu, včetně rušení přístupových práv, čímž účinně eliminuje možnosti pozdějšího zneužití informací společnosti. Vedení společnosti bude vždy přesně vědět, kdo a kdy s danými informacemi nakládal. Bude proto mít podklady pro případný spor či postih. V případě výskytu bezpečnostního incidentu, bude tento řádně dokumentován a budou definovány závazné postupy jeho řešení.

Pokud dojde k bezpečnostnímu incidentu včetně živelné pohromy, nebo cíleného útoku, budou následky minimální. Společnost má totiž díky zavedení systému bezpečnosti informací ISMS připraveny postupy pro rychlou obnovu všech svých činností.

4.5 Postup zavádění ISMS

K úspěšnému zavedení ISMS je podle ISO/IEC 27001 nutné aby organizace ustanovila, zavedla, provozovala, monitorovala, přezkoumávala, udržovala a nadále zdokonalovala tento systém, a to v souladu s modelem PDCA a normou ISO/IEC 27001. Pro úspěšné zavedení ISMS v organizaci je nutno podle (7) učinit následující kroky:

Etapa plánuj – ustanovení ISMS

- ***Definice rozsahu ISMS***

  V této části se určí rozsah a hranice, ve kterých je ISMS uplatňováno. Nejprve je potřeba získat dostatek informací, nebo provést úvodní analýzu, ze které vyplyne, které části organizace je nutno chránit. ISMS nemusí vždy pokrývat celou organizaci.

- ***Definice politiky ISMS***

  Dalším krokem je stanovení politiky ISMS. Jde o rozsahem krátký, ale významově důležitý dokument, který prezentuje zájem vedení organizace o řízení bezpečnosti informací a definuje klíčové zásady bezpečnosti. Dokument musí být schválen vedením a také s ním musí být seznámeni všichni zaměstnanci. Bez podpory vedení není implementace, provoz a údržba ISMS reálná. (12)

- ***Postupy pro řízení rizik***

  Řízení rizik je základem každého systému řízení bezpečnosti informací a podstatným způsobem ovlivňuje efektivitu fungování celého ISMS. Nezbytnými kroky pro systematické řízení rizik je:

  - Výběr vhodné metody hodnocení rizik
  - Provedení analýzy rizik
  - Návrh způsobů řízení rizik

- ***Souhlas vedení organizace s opatřeními a zbytkovými riziky***

  V této části vedení odsouhlasí navrhnutá opatření pro snižování rizik a přebírá na sebe zodpovědnost za zbytková rizika. Pokud k souhlasu nedojde, je potřeba opatření upravit.

- ***Prohlášení o aplikovatelnosti***

  Je důležitým dokumentem, který zdůvodňuje výběr jednotlivých opatření a zachycuje matici vztahů mezi hrozbami a jednotlivými opatřeními navrhnutými pro jejich účinné a efektivní snižování. Je z něj jasně patrné, která opatření budou v dané organizaci přijata, a která ne.

Etapa dělej – <u>zavádění a provoz ISMS</u>

- ***Plán zvládání rizik***

  Tento dokument popisuje veškeré činnosti spojené s ISMS jejich potřebné zdroje. Jednoznačně určuje osobní odpovědnosti za provádění plánovaných činností. Východiskem pro tento plán jsou především výsledky řízení rizik (zdokumentované ve zprávě o hodnocení rizik a prohlášení o aplikovatelnosti) a dále podněty získané pravidelným vyhodnocováním stavu ISMS vedením organizace. Plán zvládání rizik obsahuje výčet činností, aktivit a projektů vedoucích k potřebnému snižování bezpečnostních rizik.

- ***Příručka bezpečnosti informací***

  Příručka bezpečnosti slouží k podpoře prosazování ISMS a definuje dílčí procesy i postupy, které zajišťují efektivní prosazení bezpečnostních opatření. Struktura tohoto dokumentu byla popsána v kapitole 2.2.1.

- ***Prohlubování bezpečnostního povědomí zaměstnanců***

  Je potřeba zajistit promítnutí všech definovaných pravidel a postupů do skutečného chování odpovědných pracovníků a uživatelů. Je nutné jim srozumitelně vysvětlovat bezpečnostní principy a pravidla a seznamovat je s bezpečnostními riziky tak, aby byli schopni správně reagovat na nenadálé situace a hrozby. Tak je možno zajistit větší odolnost nejslabšího článku v řetězci ISMS, kterým je vždy lidský faktor.

- ***Měření provozu ISMS (indikátory a metriky prokazující účinnost ISMS)***

  Zavádí pravidelné sledování objektivních údajů o skutečném fungování systému řízení bezpečnosti. Využívá se k tomu sada ukazatelů pro oblasti finanční, personální a technické.

- ***Řízení zdrojů, dokumentace a záznamů ISMS***

  Jde o poslední krok etapy zavádění ISMS a vyžaduje provádění všech činností řízeným a dokumentovaným způsobem. Je nutné o každém kroku shromažďovat podklady pro další fázi, tedy monitorování. Cílem je tedy vytvoření pravidel pro tvorbu, schvalování a aktualizaci dokumentace řízení bezpečnosti. Současně je důležité vytvářet záznamy o všech provedených úkonech včetně identifikace osoby, která úkon provedla, kdy a kde byl realizován.

  Z pohledu zdrojů je potřeba sledovat, zda potřeby ISMS pokrývá odpovídající množství lidských, finančních a technologických zdrojů a účelně tyto zdroje řídit.

Etapa kontroluj – monitorování a přezkoumání ISMS

- ***Monitorování a provádění kontrol***

  Tento krok zahrnuje vykonávání nezbytných kontrol a testů, které poskytují zpětnou vazbu, nezbytnou pro fungování ISMS. Je potřeba dohlížet na to, zda bezpečnostní opatření naplňují očekávání, která do nich byla při zavádění vkládána. Součástí je také detekce chyb a zaznamenávání úspěšných i neúspěšných pokusů o narušení bezpečnosti. Výsledky těchto měření jsou podnětem pro přehodnocení výsledků hodnocení rizik.

- ***Interní audity ISMS***

  Zajišťují nezávislý pohled na fungování ISMS a jsou taktéž cennou zpětnou vazbou.

- ***Přezkoumání ISMS vedením***

  Podněty a připomínky k fungování ISMS získané během jeho monitorování slouží pro přezkoumání ISMS vedením organizace. Interval tohoto přezkoumání by neměl přesahovat jeden rok. Výstupem bývá zpráva o stavu ISMS, která shrnuje, co v systému funguje dobře a je možné se o tyto části opírat, a zároveň rozebere skutečnosti, které optimálně nefungují a je nutné je nadále zlepšovat.

Etapa jednej – údržba a zlepšování ISMS

- ***Soustavné zlepšování ISMS***

  Důležitým prvkem zlepšování je využití pozitivní zpětné vazby a opírání se o praktické zkušenosti účastníků tohoto procesu. Nápady a podněty přicházející z praxe jsou nenahraditelné a je potřeba jejich analýze a zapracování do systému řízení bezpečnosti věnovat velkou pozornost. U všech podnětů je nutné zvážit jejich přímé i nepřímé dopady a důsledky pro organizaci a s tím související rizika.

- ***Odstraňování neshod ISMS***

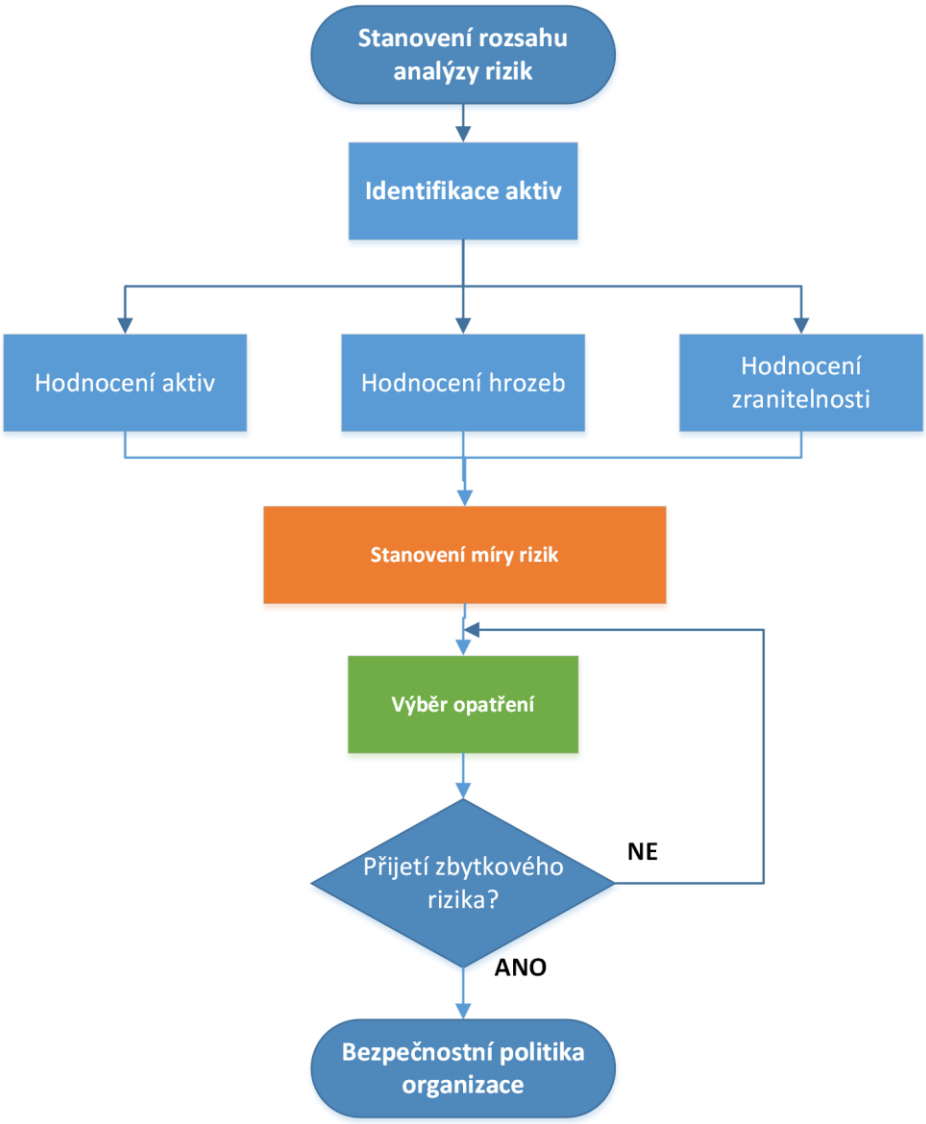
  Tento krok zavádí dvě formy odstraňování nedostatků. Opatření k nápravě, což je reaktivní forma řešení nedostatků ISMS, kdy se tento již projevil a je potřeba na něj vhodným způsobem reagovat. Naproti tomu preventivní opatření je proaktivní formou řešení nedostatků a vychází z toho, že se zjištěný problém ještě neprojevil, ale v budoucnu by mohl způsobit vážnější problémy.

Volitelným krokem po proběhnutí ISMS cyklu je **audit a certifikace**. Tu realizují nezávislé certifikační orgány. Kontrolní audit je ukončen vydáním certifikátu, který dokazuje, že byly splněny veškeré náležitosti kladené na ISMS z pohledu norem. Jeho platnost je 3 roky.

4.6 Analýza rizik

Analýza rizik je součástí procesu **řízení rizik.** Jde o a klíčový nástroj systematického přístupu k zavádění a udržování bezpečnosti informací. Cílem analýzy rizik je popis potenciálních rizik, tedy určení hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva. Na základě těchto informací je možno vybrat a prosadit vhodná bezpečnostní opatření, schopná snížit negativní účinky rizik na přijatelnou úroveň.

Analýza rizik by se měla opakovat při každé významné změně v architektuře informačního systému. Její aktualizace je rovněž dána velikostí organizace a složitosti informačního systému (6). Obecný postup analýzy rizik je uveden na následujícím obrázku:



Obrázek 6: Diagram průběhu analýzy rizik. (Vytvořeno pro potřeby DP)

Bezpečnostní politiku lze sestavit pouze na základě kvalitně provedené analýzy rizik. Tato analýza by měla rovněž předcházet jakýmkoliv finančním investicím do bezpečnosti, aby bylo zaručeno jejich maximálně efektivní využití. Analýza rizik poskytne odpovědi na otázky, co chránit, proti čemu a jakým způsobem.

4.6.1 Metody analýzy rizik

Existují dva základní principy vyjádření veličin, s nimiž se v analýze rizik dále pracuje. Jde o kvantitativní a kvalitativní metody, přičemž se použije buď jedna z nich, jejich kombinace, nebo vlastní metoda sestavená na míru dané organizaci. (6) (11)

Kvantitativní metody - využívají matematického a statistického výpočtu z frekvence výskytu hrozby a dopadu. Lze jimi rizika snadno vyjádřit v penězích, jsou tedy srozumitelné a jednoznačné. Vyjádření bývá v podobě roční předpokládané ztráty – ALE (Annualized Loss Expectancy). ALE lze vypočítat vynásobením ztráty při jednom výskytu hrozby - SLE (Single Loss Exposure) s pravděpodobností výskytu hrozby za rok - ARO (Annualized Rate of Occurrence). Platí tedy vztah: ALE = SLE × ARO. Nevýhoda těchto metod je spojená s vysoce formalizovaným přístupem. Kvantitativní metody jsou náročnější na provedení a zpracování výsledků.

Kvalitativní metody - Jsou považovány za jednodušší a rychlejší. Závisí na subjektivním posouzení odborníků. Pro popis výše dopadu, hrozeb, zranitelností a konečného rizika se používá hodnotící stupnice <1 až 10>, nebo slovní popis <nízké, střední, vysoké>, případně hodnota pravděpodobnosti <0, 1>. U těchto metod chybí vyjádření finanční hodnoty aktiva, což snižuje efektivnost kontroly nákladů.

Vlastní metoda – vlastní metodika, sestavená na základě znalostí daného prostředí přesně na míru, dle mezinárodních norem a standardů.

4.6.2 Přístupy k analýze rizik

Norma ISO/IEC 27005 uvádí několik možných přístupů k analýze rizik (3):

Základní – spočívá v aplikaci základních bezpečnostních opatření pro všechny systémy. Neproběhne zde podrobná analýza, což tento proces výrazně urychlí a zlevní, avšak nelze pomocí něj zajistit adekvátní bezpečnostní zajištění každého prvku. Bude-li základní úroveň nastavena příliš nízko nebo zbytečně vysoko, nemusí být úroveň bezpečnosti dostačující, případně na ni mohou být vynaloženy zbytečné náklady.

Neformální – využívá dlouhodobých zkušeností a znalostí jednotlivců. Úroveň míry rizik je obvykle určována kvalifikovaným odhadem. Tento přístup je relativně rychlý a finančně nenáročný. Může však dojít k opomenutí důležitých detailů, navíc může být do analýzy zanesena určitá míra subjektivity. Potíže mohou nastat i v případě, že by jednotlivec řešící analýzu od organizace odešel.

Detailní – zahrnuje následující dílčí kroky:

- identifikaci a ohodnocení **aktiv**;
- identifikaci a ohodnocení **hrozeb**;
- identifikaci a ohodnocení **zranitelností**;
- stanovení jednotlivých **rizik**.

Výsledkem těchto kroků je vztah mezi hodnotou rizika a hodnou aktiva, hrozby a zranitelnosti. Rizika se poté vyhodnotí a následně se na ně aplikují odpovídající bezpečnostní opatření tak, aby byla dosažena požadovaná bezpečnost. Výhodou detailní analýzy rizik je, že pro všechny použité systémy budou vybrána vhodná opatření. Tento přístup vyžaduje značné úsilí a je velmi náročný jak časově, tak po stránce finanční a odborné. Není vhodné používat detailní analýzu pro všechny systémy.

Kombinovaný – kombinuje nejlepší vlastnosti základního přístupu a detailní analýzy rizik. Prvotní analýza je provedena pro všechny systémy a teprve potom detailně pro systémy, které jsou klíčové pro činnost organizace. Tento přístup minimalizuje časovou náročnost při zachování maximální finanční efektivnosti. Finanční prostředky jsou vynakládány jen tam, kde jsou skutečně zapotřebí.

4.6.3 Postup při analýze rizik

Při provádění analýzy rizik je nezbytné provést níže uvedené kroky (11):

Definovat hranice analýzy rizik – vymezit ta aktiva, která budou do analýzy zahrnuta. Tento krok určuje rozsah celé analýzy. Jde o fiktivní dělicí čáru mezi aktivy organizace.

Identifikovat aktiva – vytvořit seznam (název, umístění, vlastník atd.) všech aktiv ležících uvnitř hranic analýzy rizik. Tento krok by měli v ideálním případě provádět interní zaměstnanci, protože mají o firemních aktivech nejlepší přehled a povědomí.

Ohodnotit a seskupit aktiva – ve většině případů si skutečné hodnoty aktiv a informací podnik či organizace uvědomí až tehdy, když dojde k jejich ztrátě. Proto je důležité, aby si organizace vymezily veškerá aktiva a hodnoty, jaké pro ně mají. Po tom co jsou jednotlivá aktiva identifikována, je vhodné je seskupit podle různých hledisek a vytvořit skupiny aktiv s podobnými vlastnostmi. Taková skupina pak může vystupovat jako jedno aktivum a ušetřit práci s vyhodnocováním vlivů hrozeb na jednotlivá (podobná) aktiva. Ke stanovení hodnoty aktiva lze přistupovat několika způsoby, podstatou však je, že hodnota aktiva se posuzuje na základě velikosti škody, jež by mohla způsobit ztráta nebo zničení aktiva. V tomto procesu je zohledňována pořizovací cena aktiva, ale například i výnosy z daného aktiva. Do jeho hodnoty se také promítá skutečnost, do jaké míry je podnik na daném aktivu závislý. (3) (7) (11)

Identifikovat hrozby - v tomto kroku analýzy rizik se vyhledávají hrozby, pro které musí být v dalších krocích následně nalezeno odpovídající protiopatření. Výběr možných hrozeb je nutno provádět tak, aby tyto hrozby vždy působily na jedno, či více identifikovaných aktiv. Příklady hrozeb lze získat z různých zdrojů, především z katalogu hrozeb ISO/IEC 27005, oborových zkušeností, případně z provedených analýz, nebo softwaru (Delphi, CRAMM apod.). Hrozby je možné v podniku identifikovat také pomocí brainstormingu. Je vhodné je rozlišovat podle výskytu na interní / externí a přírodní / fyzické.

Ohodnotit hrozby a zranitelnosti – s ohledem na hodnotu a význam dotčených aktiv se určí výše dopadu na aktiva a následná výše škody, kterou by hrozba mohla organizaci způsobit. Na základě zkušeností se určí pravděpodobnost, se kterou se daný scénář může uplatnit. Dalším krokem je stanovení míry zranitelnosti. Ta se určí na základě existujících

bezpečnostních opatření. Posuzuje se míra jejich účinnosti vůči definovanému scénáři. (6) (11)

Stanovit výslednou míru rizika - výše rizika je odvozena z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva. Stanovení výsledné hodnoty rizika je obtížné, protože se pro hodnocení používají často neměřitelné, nebo jen velmi těžce měřitelné veličiny. Lze se setkat s pojmy jako malé, střední, nebo vysoké riziko. Při kvantifikaci rizika je také třeba počítat s pravděpodobností výskytu jevu, kdy jev pravděpodobnější dostává od hodnotitele vyšší hodnotu rizika. Hodnota rizika vyjadřuje velikost, jakou míru zranitelnosti zneužila hrozba.

Matematicky lze riziko vyjádřit několika způsoby:

- Tří faktorový přístup, který je definován jako:

$$R = A \times H \times Z$$

kde R je míra rizika, A hodnota aktiva, H pravděpodobnost hrozby, Z zranitelnost.

- Dvou faktorový přístup, který je definován jako:

$$R = PI \times D$$

kde R je míra rizika, RI pravděpodobnost incidentu, D dopad. (5)

4.6.4 Softwarové nástroje a metody podporující analýzu rizik

K praktickému provádění analýzy rizik je vytvořena poměrně velká řada softwarových nástrojů, z těch nejznámějších jsou to například (11):

Metoda **COBRA** – pro analýzu využívá expertní systém. Odborník identifikuje hrozby a stanoví rizika, na základě toho systém zpracuje řešení, ze kterých se pak uskuteční výběr protiopatření.

Metoda **CRAMM** (CCTA Risk Analysis and Management Methodology) – velmi používaná metoda od společnosti RAC. Na základě seznamu hrozeb a zranitelností lze s její pomocí zpracovat analýzu rizik. Metoda řeší jak implementaci, tak audit. Její výhodou je jednoznačně rychlost provedení analýzy, stanovení nejrizikovějších částí systému a navrhnutí bezpečnostních opatření pro snížení rizik.

Metoda **Delphi** – metoda kvalitativní analýzy rizik, prováděna formou expertního odhadu. K hodnocení používá seznam otázek, které jsou konzultovány s příslušnými představiteli. Metoda klade nižší nároky na zdroje a zohledňuje specifika posuzovaného systému.

4.6.5 Druhy rizik

Každé riziko má neblahý vliv na finanční oblast organizace, je tedy nutné rozlišovat, o jakou úroveň ohrožení se jedná. Úrovně rizik mohou být podle (6):

Nízké – v tomto případě je riziko pro podnik obvykle akceptovatelné, jeho působením nedochází k téměř žádným citelným ztrátám. Přesto je však nutné jej nadále monitorovat a rozhodně nesmí být ignorováno. Zavedení efektivního opatření je velmi nesnadné, přičemž riziko je minimalizováno jen nepatrně. Opatření proti nízkým rizikům je možno zavádět řádově v měsících.

Střední – zde je již nutností zavést opatření, která ovšem minimalizují riziko jen z části. Náklady na opatření by neměly převýšit hodnoty ohrožených aktiv. Opatření bývají zaváděna řádově v týdnech.

Vysoké – jde o úroveň, kdy je nezbytné co nejdříve přijmout taková opatření, aby došlo k výraznému snížení úrovně rizika. Zavedení probíhá řádově ve dnech.

Kritické – probíhající proces musí být ukončen do doby, než budou zavedena opatření, která toto riziko sníží. Navrhují se jednoduchá a rychle aplikovatelná opatření, která je možno zavést během několika hodin.

Určité kombinace hodnoty dopadu a pravděpodobnosti hrozby vedou ke stejným úrovním rizika. Je vhodné tuto skutečnost zohlednit ve fázi zvládáni rizik, protože je rozdíl, zda u rizika vyšla úroveň "střední" z důvodu vysoké pravděpodobnosti hrozby, nebo vysoké hodnoty aktiva. V procesu snižování rizika je třeba brát v úvahu, že riziko nikdy zcela neeliminujeme. Často nastane situace, že zavedením opatření vzniknou další typy rizik. Je nutné výběru opatření věnovat náležitou pozornost.

4.7 Zvládání rizik

Závěrečným krokem efektivního řízení rizik je navrhnutí a prosazení vhodných forem ochrany. Na základě zjištěných bezpečnostních potřeb a stanovení priorit je nutné vybrat vhodná bezpečnostní opatření, která umožní zjištěná rizika efektivně snižovat. Pro zvládání rizik se nejčastěji využívá katalog opatření definovaný normou ISO/IEC 27002. V případě potřeby je možné doplňovat bezpečnostní opatření i nad rámec těchto obecných doporučení.

Je potřeba, aby s návrhem bezpečnostních opatření souhlasilo vedení organizace. Dalším krokem je akceptace zbytkových rizik vedením. V případě, že vedení zjistí, že

výsledky řízení rizik nevedou k požadované úrovni bezpečnosti, je možné včas upravit návrh bezpečnostních opatření. Souhlas se zbytkovými bezpečnostními riziky pak představuje souhlas vedení s určitou mírou rizika při ochraně informací v organizaci.

Řízení rizik je cyklický proces, který je potřeba provádět po celou dobu životnosti systému řízení bezpečnosti informací v organizaci.

4.7.1 Způsoby zvládání rizik

Bude-li úroveň výsledného rizika střední až kritická, mělo by se usilovat o jeho snížení. Ke snížení rizika může být využito několik způsobů, z nichž nejvíce se používá akceptace a redukce rizika. Způsoby snižování rizik zobrazeny na Obrázek 7 a v Tabulka 1. Podle (6) rozlišujeme následující metody:

Monitorování rizika – přijmou se minimální doporučené bezpečnostní opatření. Doporučuje se v případě, že analýza rizik neukázala žádná významná rizika, která by citlivá aktiva organizace ohrožovaly.

Akceptace rizika – jde o nejpoužívanější metodu v případě, že dopad na aktivum je takřka zanedbatelný. Management toto riziko vědomě přijímá.

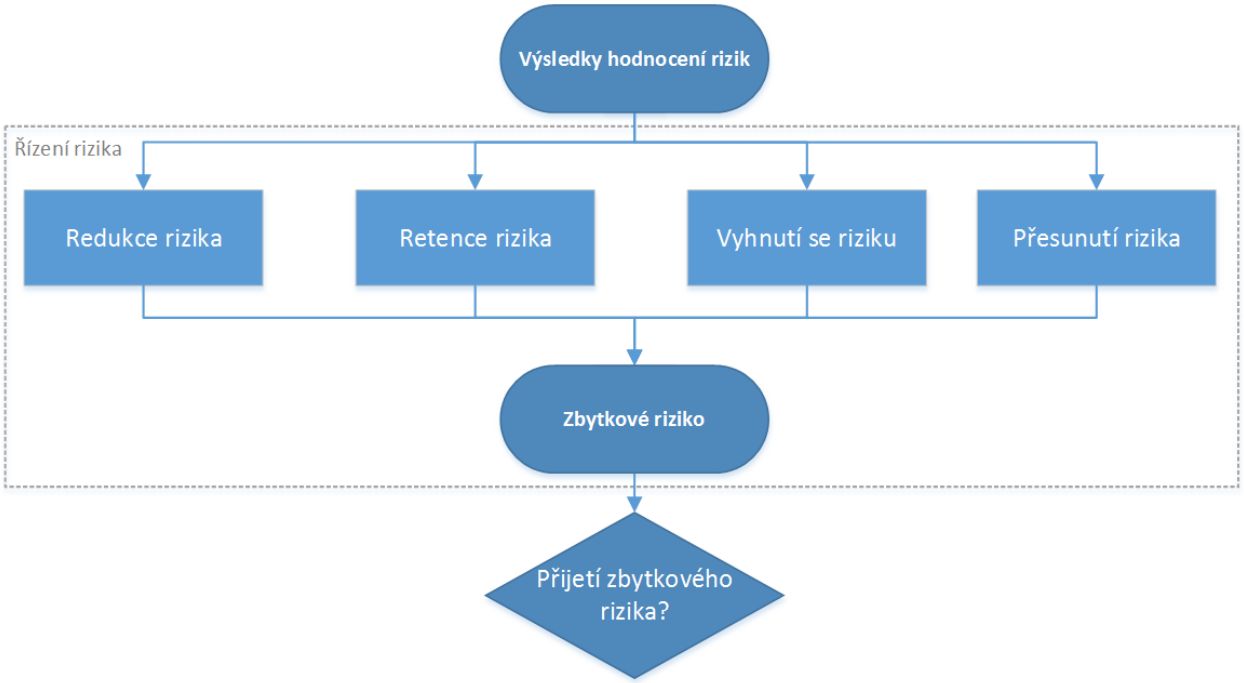
Redukce rizika – tento způsob spočívá ve snížení rizika na požadovanou hodnotu vhodným opatřením. Redukce rizika se používá v případech vysokého výskytu rizik hrozbě výraznějších ztrát.

Pojištění proti riziku – je možné pojistit jak movitý a nemovitý majetek, tak samotné zaměstnance. Tento způsob však riziko nesnižuje, jen pokrývá možné následky. Je vhodné v případě, že výskyt bezpečnostních incidentů není pravděpodobný, ale pokud by k němu došlo, měl by kritický vliv na chod organizace.

Transfer rizika – jde o přenos odpovědnosti na jiný subjekt. To může být provedeno pomocí outsourcingu nebo společného partnera. Používá se, pokud je riziko hrozby zničující a pravděpodobnost výskytu je nízká.

Vyhnutí se riziku – tato metoda je používána v případech, kdy je prováděna nějaká změna, po které dané riziko zmizí.

Ignorování rizika – nejnebezpečnější případ, kdy se o riziku vůbec neví.



Obrázek 7: Řízení rizika. Podle (3).

	Vysoká pravděpodobnost	Nízká pravděpodobnost
Vysoká tvrdost	Vyhnutí se riziku, redukce	Pojištění
Nízká tvrdost	Retence a redukce	Retence

Tabulka 1: Přístup ke snižování rizik. Podle (11).

4.7.2 Výběr bezpečnostních opatření

Bezpečnostní opatření, jsou ve vzájemném vztahu a účelem je jejich kombinování s cílem nížení rizika na požadovanou hodnotu. Úkolem managementu je zvolit příslušná opatření s přihlédnutím k pořizovacím nákladům a efektivitě. (6)

Efektivita určuje kvalitu opatření a jeho schopnost snižovat identifikované hrozby nebo zranitelnosti. **Ekonomičnost** určuje vztah mezi náklady, které je nutné vynaložit na pořízení a provoz určitého bezpečnostního opatření vůči hodnotě daného aktiva. Při hodnocení jednotlivých variant je nutné si uvědomit, že i samotná opatření se mohou stát terčem útoku. Je proto vhodné při výpočtu nákladů každého opatření zahrnout i ty, které souvisí s jejich ochranou či údržbou. Dalšími faktory, které mohou kromě efektivity a ekonomičnosti ovlivnit výběr výsledného opatření jsou technická a časová náročnost na jejich zavedení.

4.8 Oblasti ISMS

Norma ISO/IEC 27001 pokrývá svou působností řadu různých oblastí, jak znázorňuje Obrázek 8, a pro každou z nich uvádí v příloze A vhodná opatření. Konkrétní způsoby zavádění opatření pak rozvádí norma ISO/IEC 27002.

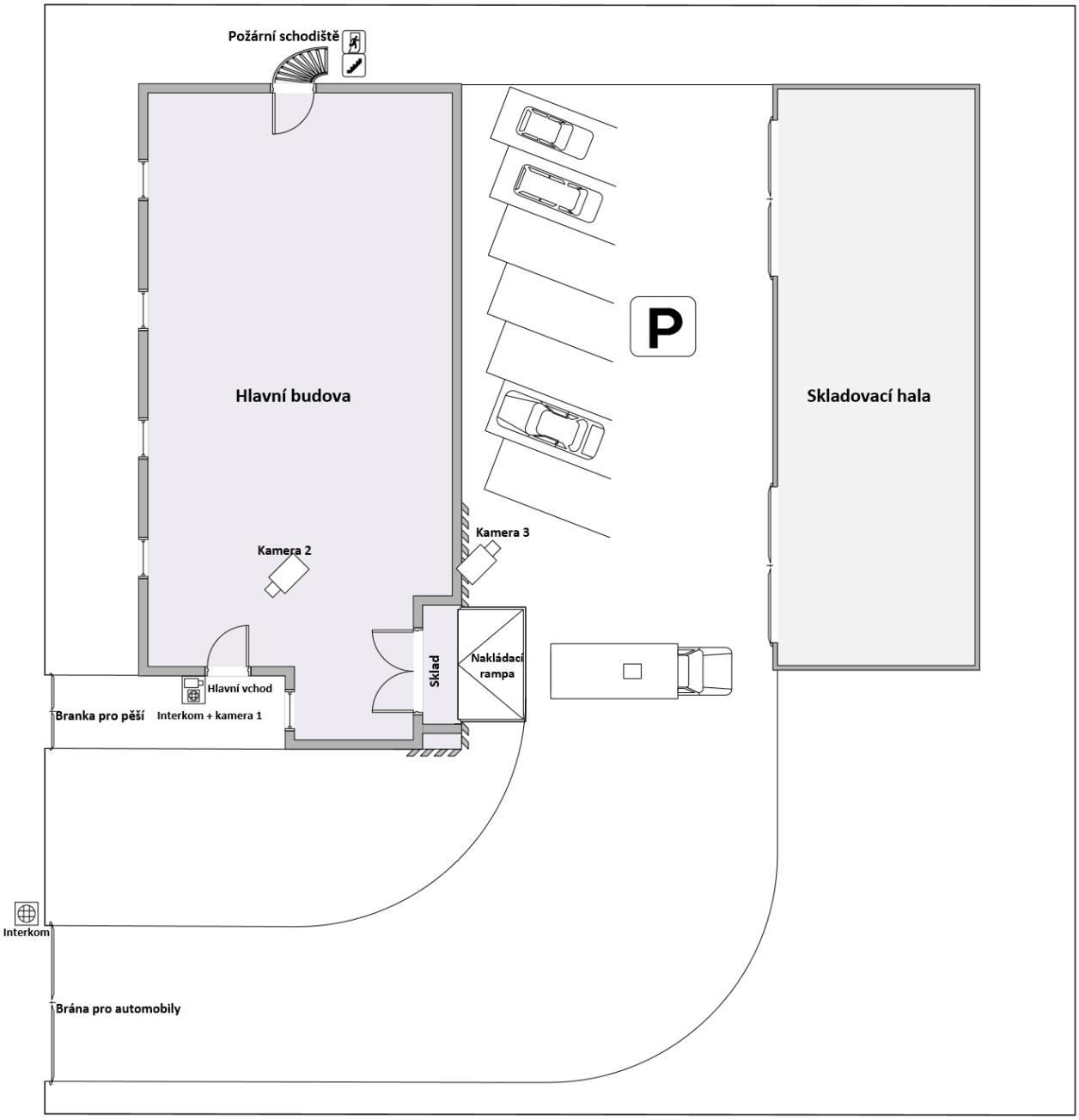
Obrázek 8: Oblasti ISMS. (9) (1)

Norma nepřikazuje, která opatření musí být bezpodmínečně aplikována, ale ponechává rozhodnutí na organizaci. Vhodná opatření jsou vybírána na základě hodnocení rizik a jejich implementace je závislá na konkrétní situaci. Cílem není implementovat vše, co norma popisuje, ale spíše naplnit všechny aplikovatelné cíle opatření. Tento přístup zajišťuje, že norma je široce aplikovatelná a dává uživatelům velkou flexibilitu při implementaci. Nicméně toto přináší obtíže při certifikaci, kdy může být složité posoudit, zda jsou aktuální bezpečnostní opatření plně v souladu s normou. (7)

5 Analýza současného stavu

5.1 Situační analýza

Společnost sídlí na okraji města ve vlastní tří patrové budově s přilehlým parkovištěm a skladovací halou. Celý pozemek je oplocen a vybaven bránou pro automobily i pro pěší. Na budově je nainstalován kamerový systém, který monitoruje parkoviště a přístupové cesty. Dopravní spojení je zajištěno silnicí 1. třídy v těsném sousedství pozemku.

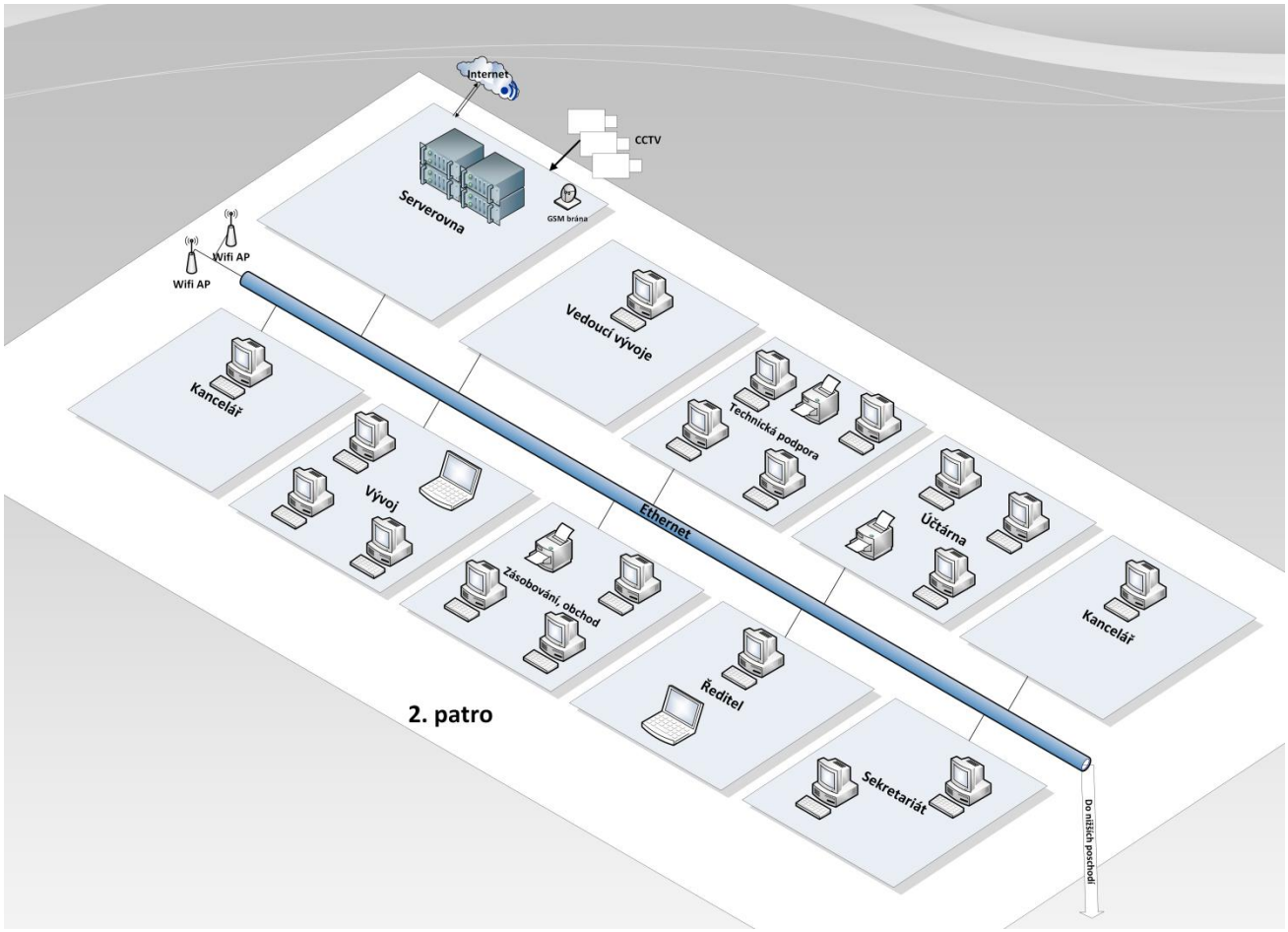


Obrázek 9: Nákres budov a celého pozemku. (Vytvořeno pro potřebu DP)

Přístup do budovy: U brány i u vstupních dveří jsou nainstalovány snímače přístupových čipů zaměstnanců a také zvonek s hlasovým zařízením (interkomem) sloužící pro návštěvy.

V přízemí se nachází nakládací rampa pro kamion, sklad materiálu a zboží připraveného pro expedici a dílna včetně SMT osazovací linky. V prvním patře budovy je druhá dílna a sklad materiálu. Předmětem zájmu této práce je pak především druhé nadzemní patro, ve kterém se nacházejí kanceláře vedení společnosti, účtárna, konferenční místnost, serverovna a vývojové oddělení.

Okolní krajina je kopcovitého charakteru a hranicí pozemku protéká potok. Díky dostatečnému spádu krajiny se však pozemek nenachází v rizikové oblasti z hlediska povodní.



Obrázek 10: Schéma druhého patra. (Vytvořeno pro potřebu DP)

5.2 Zabezpečení objektu

Celý pozemek okolo budovy je oplocen. Přístupová místa jsou branka pro pěší (ta je během pracovní doby odemčená) a brána pro automobily, kterou si zaměstnanci otevírají RFID čipem, návštěvy pak využijí interkom. Budova má jeden hlavní vchod, který je opatřen zařízením pro komunikaci doplněným kamerou a také snímačem RFID čipů zaměstnanců. Kamera u vchodu je jednou ze tří bezpečnostních kamer, které jsou aktivní 24 hodin denně. Záznam se ukládá na server a přímý přenos videa je dostupný na firemní síti. Snímače čipů jsou provázány s docházkovým systémem a údaje jimi zaznamenané slouží jako podklad pro výpočty mezd zaměstnanců. Tento systém rovněž umožňuje povolit případně odepřít jednotlivým zaměstnancům přístup do vybraných prostor.

Prostory uvnitř budovy i ve skladovací hale jsou pro případ neoprávněného vniknutí do objektu vybaveny elektronickým zabezpečovacím systémem kanadského výrobce Paradox. Každé patro budovy i hala má vlastní nezávislý okruh střežený pohybovými čidly. Tento systém se aktivuje po konci pracovní doby v daném sektoru. Zabezpečovací systém je napojen na pult centrální ochrany místní bezpečnostní služby. Propojení je z bezpečnostních důvodů (přerušení kabeláže útočníkem) provedeno bezdrátově. Anténa, která spojení zajišťuje je umístěna v serverovně. Serverovna je uzamčená místnost bez oken umístěná ve druhém nadzemním podlaží, což z ní dělá nejbezpečnější místo celé budovy.

Ze zadní strany budovy je kovové požární schodiště, na které vedou dveře z každého patra. Tyto dveře lze otevřít pouze zevnitř a dle platné legislativy je nutné, aby byly během pracovní doby odemčené. Budova je vybavena také několika požárními čidly na rizikových místech a jedno je umístěno také v serverovně. Případný požární poplach je stejně jako pokus o neoprávněné vniknutí odeslán na pult centrální ochrany.

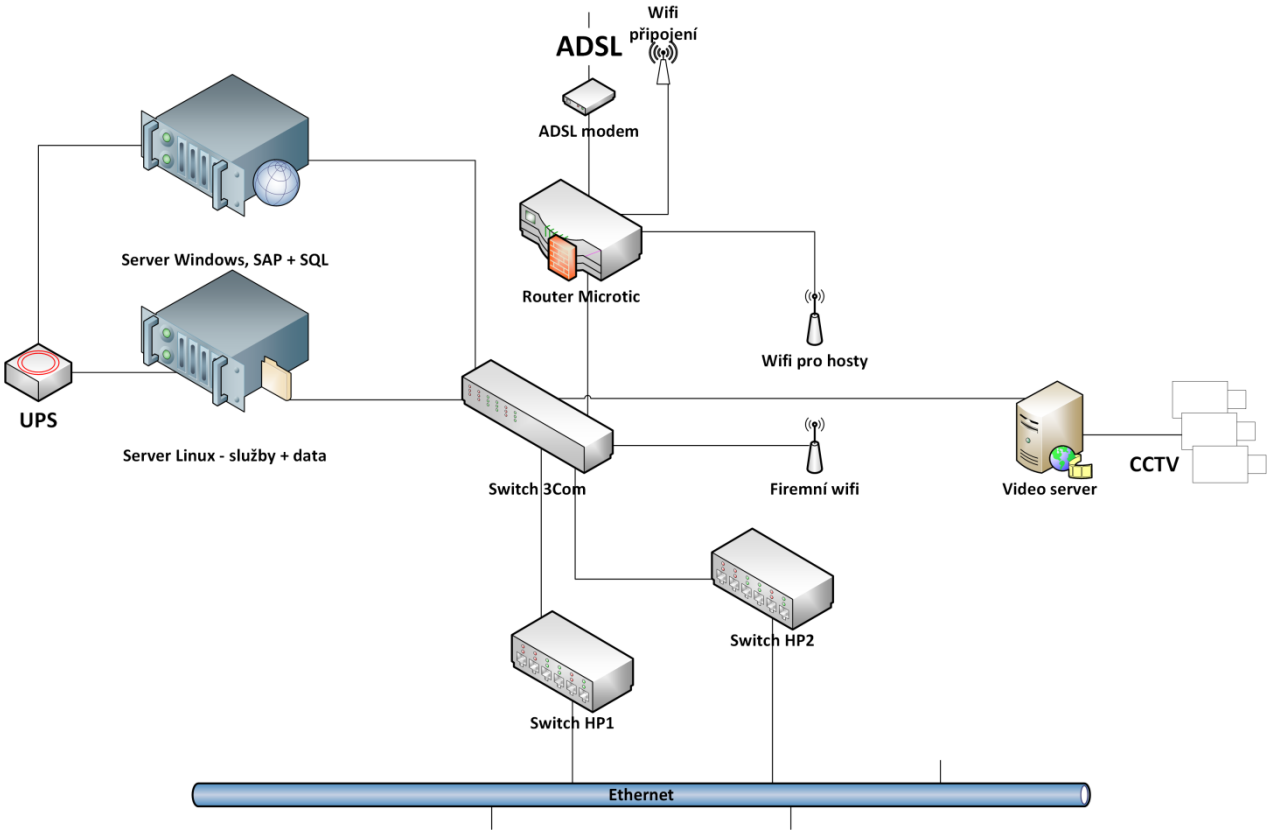
5.3 ICT infrastruktura

Rozvody síťové kabeláže byly instalovány stavební firmou při stavbě budovy v roce 2004. Strukturovaná kabeláž je vedena v kabelových žlabech, ve zdech a nad stropními podhledy. V každé místnosti je po obvodu okolo pěti zásuvek pro RJ-45 kabely. Zásuvky jsou po dvou konektorech, z nichž jeden se využívá pro připojení síťových zařízení a druhý pro telefon. Kabelové svazky z jednotlivých pater a místností vedou do patch panelů v serverovně. Zde je také umístěna digitální telefonní ústředna s GSM bránou, kam vedou kabely z telefonních zásuvek jednotlivých místností.

5.3.1 Serverovna

Mezi nejdůležitější vybavení serverovny patří tři servery, tři switche, router, ADSL modem, telefonní ústředna s GSM bránou a záložní zdroje napájení. Na jednom serveru běží pod operačním systémem Windows Server 2003 firemní informační systém SAP Business ONE, SQL Server a výrobní systém. Druhý server se systémem Linux Debian slouží především jako poštovní server a datový sklad. Běží na něm docházkový systém DoSys. Úlohou posledního, video serveru, je digitalizovat video ze tří analogových bezpečnostních karet, ukládat záznam (uchovává se cca 5 dní) a streamovat video do podnikové sítě LAN. Na tomto stroji však běží Windows XP, nejedná se tedy o server v pravém slova smyslu. První dva servery jsou pro chod firmy životně důležité a jejich napájení je proto jištěno záložními zdroji. Veškeré vybavení serveru je uloženo v kovovém racku 19” o výšce 24U.

Ve firmě byla v nedávné době nainstalována dvě Wi-Fi přípojná místa. Jedno slouží pro zaměstnance a dá se pomocí něj připojit do lokální sítě, druhé je určeno pro návštěvy a slouží pouze pro připojení k internetu. Firma využívá dvě formy připojení k internetu. Primární je ADSL linka od poskytovatele O2. V případě výpadku se přechází na Wi-Fi připojení od místního poskytovatele internetu.



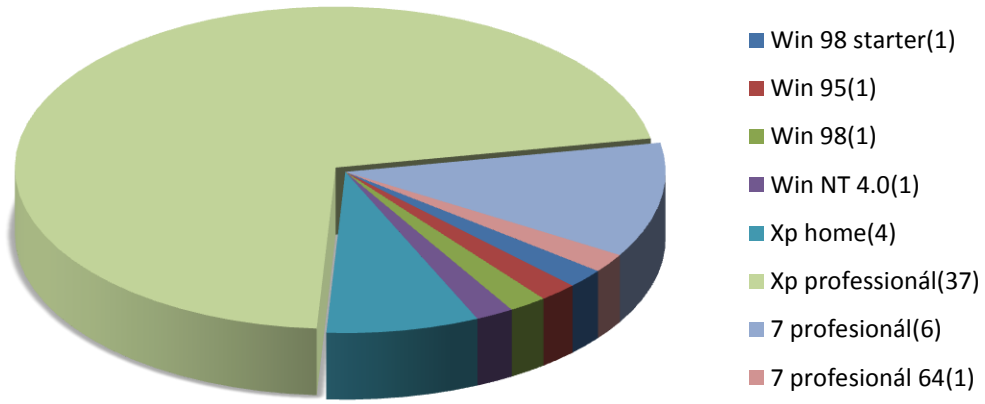
Obrázek 11: Schéma serverovny. (Vytvořeno pro potřebu DP)

Tabulka 2: Specifikace vybavení serverovny

Zařízení	Typ	Parametry	Počet
Router	Microtic RB2011 UAS-RM	5x 100Mbit/s, 5x 1Gb/s. RouterOS Level 5, podpora IPv6. Přidělování adres, routování, firewall.	1
Switch	3com 2816-SFP plus	16x 10/100/1000 port.	1
Switch	HP V1910V6	48x 10/100/1000 port. Funkce správy IMC, Web browser, SNMP Manager	2
Server	Fujitsu Primergy RX100 S6 (1U)	Xeon X3450 4x 2,66 GHz, 4GB DDR3, 2x1TB HDD. Linux Debian 6.	1
Server	Fujitsu Primergy TX150 S6 (Tower)	XEON 3360 4x2,83GHz, 4GB DDR, 2x 300GB SAS DSS. Windows Server 2003.	1
Tel. ústředna	Nexspan Astra	Digitální telefonní ústředna připojená ke GSM bráně.	1

5.3.2 Pracovní stanice

Do sítě LAN je připojeno 52 stanic. Z nich 20 slouží pro potřeby výroby, zbylých 32 počítačů je možno označit jako pracovní stanice zaměstnanců. Jedná se o v průměru 5 let staré počítače různých výrobců. Na počítačích se nacházejí různé verze operačního systému Microsoft Windows, podle stáří konkrétní stanice. Zastoupení jednotlivých systémů v podniku je graficky vyjádřeno na Obrázek 12.



Obrázek 12: Zastoupení operačních systémů v podniku

Většina stanic je vybavena systémem Windows XP Professional. Z nainstalovaných programů je to pak nejčastěji kancelářský balík MS Office (verze 2003 – 2010) a následně specializované designérské a vývojové programy, odpovídající účelu stanice. Můžeme jmenovat například: Corel Draw, Autocad LT, Eagle, Solid Works, Code Warrior. Záložní napájecí zdroje jsou instalovány pouze u počítačů v účtárně a to z důvodu provádění kritických operací v informačním systému z hlediska nutnosti zachování integrity dat.

5.3.3 Ostatní ICT vybavení

Mezi ostatní ICT vybavení firmy je možno zařadit síťové tiskárny v počtu 5 kusů, notebooky, čtečky čárových kódů (ve výrobě), osazovací automaty a další zařízení jako scannery, dataprojektory a terminály docházkového systému.

Firma nedisponuje vlastním IT oddělením. Instalaci serverů, upgrade pracovních stanic a vzdálenou správu provádějí najaté externí subjekty. Ve firmě je však IT správce, který obsluhuje servery a řeší problémy menšího rozsahu, jak na síťových aktivních prvcích (zapojení a evidence patch panelů), tak na pracovních stanicích uživatelů, případně i na serveru.

5.4 Externí subjekty

5.4.1 Bezpečnostní agentura

Analyzovaná společnost má smluvní vztah s bezpečnostní agenturou, jejíž jméno zde záměrně neuvádím z důvodu snadné lokalizace popisované společnosti. Jde o místní agenturu, působící zde od roku 1997. Agentura je členem asociace soukromých bezpečnostních služeb České Republiky a od roku 1999 je držitelem certifikátu ISO 9001 - "Fyzická ostraha majetku a osob" a také certifikátu Národního bezpečnostního úřadu, které společnosti umožňuje přístup k utajovaným informacím stupně "vyhrazené". V roce 2005 společnost investovala do pultu centrální ochrany (PCO), který provozuje a také do privátní rádiové sítě. Privátní rádiová síť je v současné době nejbezpečnějším a nejrychlejším způsobem přenosu informací z objektu na PCO. Kontrola objektu probíhá každých 5 minut a samotný poplach se na PCO přenese do 3 sekund. Navíc odpadají poplatky za datové, případně telefonní přenosy operátorům, jak je tomu u běžných systémů.

Smluvní vztah: V případě poplachu přijedou pracovníci agentury a zajistí místo. Pokud došlo ke vniknutí, volají polici ČR a informují majitele firmy. V opačném případě kontaktují a přivolají majitele. Agentura nemá přístup do budovy společnosti.

5.4.2 Úklidová firma

Druhým externím subjektem souvisejícím s fyzickou bezpečností objektu je najatá úklidová firma. Ta přístup do budovy má. Uklízečka vlastní univerzální klíč od všech kanceláří, kde provádí úklid na začátku pracovní doby. Do budovy se však sama mimo pracovní dobu nedostane.

5.5 Aktuální úroveň bezpečnosti informací

5.5.1 Dotazník určený zaměstnancům

Pro lepší zmapování reálného stavu zajištění bezpečnosti informací a bezpečnostního povědomí zaměstnanců společnosti byl sestaven anonymní dotazník, který tvoří přílohu 1 této práce.

Dotazník byl vytvořen pomocí služby Google Forms a následně rozeslán prostřednictvím firemní elektronické pošty celkem 25 administrativním a vývojovým pracovníkům. Ve zprávě nebylo záměrně specifikováno, k jakému účelu budou získaná data využita, a byla zdůrazněna anonymita. Tuto strategii jsem volil proto, že ve společnosti nejsou dosud zavedeny žádné směrnice v oblasti IT technologií a využívání firemní sítě. To dává zaměstnancům značnou svobodu, minimální dohled a téměř žádné postihy. Dá se tedy předpokládat, že jim aktuální stav vyhovuje a pokud by z dotazníku bylo patrné, že zkoumá slabá místa v oblasti bezpečnosti informačních technologií pro budoucí zavedení ISMS, mohli by záměrně podávat zkreslené informace. Dotazník obsahuje celkem 18 otázek, na které se odpovídá volbou jedné z možností, respektive zatrhnutím kombinace možností.

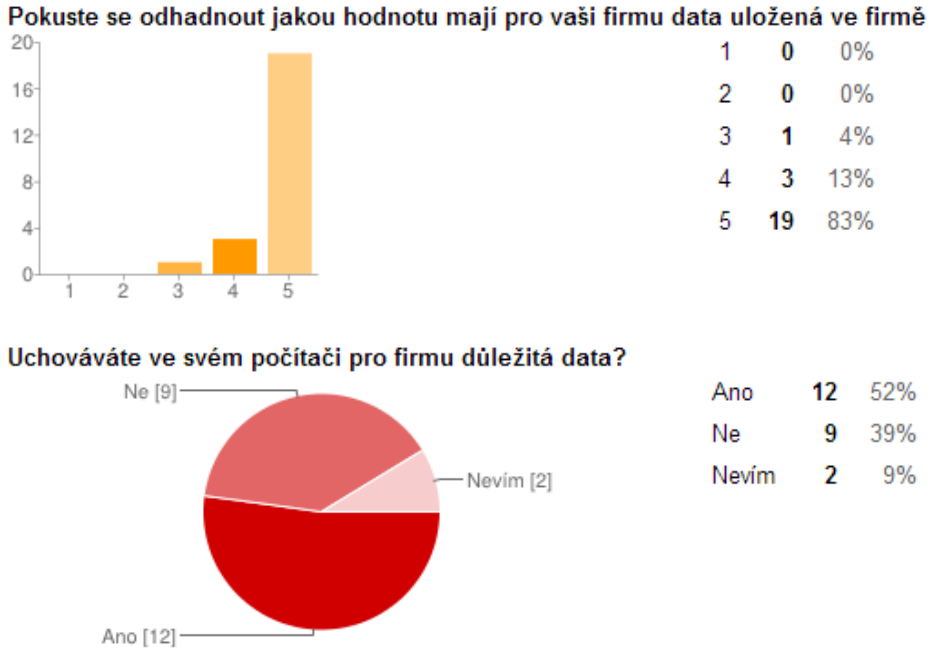
Otázky pokrývaly tato témata:

- Ztráta dat
- Ochrana počítače heslem
- Uchovávání důležitých firemních dat
- Neoprávněná modifikace dat
- Způsob výměny dat mezi pracovníky
- Hodnota firemního HW, SW, Informací
- Firemní politika bezpečnosti IT
- Školení bezpečnosti IT
- Zálohování
- Přístup k firemnímu IS
- Přístup k internetu
- Dohled zaměstnavatele nad internetovou aktivitou
- Instalace programů na pracovní stanice
- Úroveň zabezpečení informací uvnitř i vně firmy
- Zaznamenané bezpečnostní incidenty

Celkem bylo přijato 23 korektně vyplněných dotazníků, což považuji za velmi dobrý výsledek (92%) vzhledem k anonymitě a tedy i dobrovolnosti tento dotazník vyplnit.

5.5.2 Závěry z výsledků dotazníku

Kompletní grafické vyhodnocení jednotlivých otázek je přiloženo k práci (Příloha 2). Zde bych jen stručně shrnul některé poznatky plynoucí z vyhodnocených dat.



Obrázek 13: Ukázka grafického vyhodnocení jednotlivých otázek - viz příloha 2

Z výsledků průzkumu vyplývají tyto skutečnosti:

Čtvrtina zaměstnanců již někdy přišla o svá data. Třetina zaměstnanců svůj počítač vůbec nechrání heslem. Většina z nich však uchovává pro firmu důležitá data. Nejrozšířenější způsob sdílení dat mezi zaměstnanci je firemní email, dále pak firemní datový server a papírová forma dokumentů. Zaměstnanci správně vyhodnotili, že pro jejich firmu mají nejvyšší hodnotu informace, následně softwarové a nakonec hardwarové vybavení. Avšak význam hardwaru výrazně nadhodnotili. Průměrně mu přiřadili hodnotu 3,8 z maxima 5. U softwaru potom hodnotu 4 a u Informací 4,8. Zajímavým poznatkem je, že téměř polovina zaměstnanců si myslí, že v podniku existuje nějaká směrnice upravující politiku bezpečnosti informací a pravidla pro chování v síti. Zbytek správně uvedl, že neexistuje, případně že

neví. 80% zaměstnanců neví, jestli je jejich aktivita na internetu monitorována zaměstnancem, zbytek odpověděl, že není. Úroveň zajištění bezpečnosti informací uvnitř organizace hodnotí zaměstnanci jako průměrnou, úroveň vnějšího zabezpečení informačních aktiv pak jako nadprůměrnou. Každý zaměstnanec se setkal s nějakým bezpečnostním incidentem. Téměř všechny postihl výpadek elektrického proudu a nedostupnost firemní sítě. Třetina z nich se potom setkala se zahlcením emailové schránky spamem a čtvrtina s počítačovým virem. Nejasná je pro zaměstnance problematika instalace programů na firemní počítače. Rozdělili se na 3 obdobně velké skupiny, kdy zaměstnanci jedné odpověděli, že můžou sami instalovat jakékoliv programy, druhé že instalovat programy může jen správce sítě a poslední skupina neví, respektive zatím neměla potřebu nic instalovat. Vyšlo najevo také to, že někteří zaměstnanci nemají přístup do firemního informačního systému, ačkoliv to povaha jejich práce vyžaduje a na druhé straně tam mají přístup i zaměstnanci, kteří jej k práci nepotřebují. Stejná situace poté nastala i u další otázky týkající se přístupu k internetu. Cenné poznatky z tohoto průzkumu vezmu v úvahu při výběru opatření pro zajištění bezpečnosti informací v organizaci, a také při návrhu podoby příručky informační bezpečnosti.

5.5.3 Shrnutí stavu informační bezpečnosti v podniku

V podniku není zatím problém informační bezpečnosti systematicky řešen a neexistují závazné směrnice, ani bezpečnostní školení. Data zaměstnanců na pracovních stanicích nejsou pravidelně zálohována. Je vhodné, aby je zaměstnanci ukládali na datový server. Není zde však zavedena hierarchie přístupových práv, které by byly přidělovány skupinám uživatelů. Uživatelé mají právo číst, editovat i mazat veškeré přístupné dokumenty. Někteří uživatelé nepoužívají hesla a běžně nechávají bez dozoru stanice připojené k informačnímu systému. K neoprávněné modifikaci dat tak může dojít velice snadno a bylo by téměř nemožné odhalit viníka.

Přenosná média nejsou skladována v uzamčených zásuvkách. Nejsou evidována a často se pro přenos dat používají soukromá média pracovníků. Ty pak přenáší mimo areál firmy, kde hrozí jejich ztráta či odcizení a připojují je k neprověřeným počítačům.

Situaci nelze vyhodnotit jako kritickou jen z důvodu, že jde o menší podnik, kde se zaměstnanci, kteří pracují s ICT vybavením, navzájem znají a nemají zájem podnik poškodit. Pravidelně se zálohují alespoň data serveru, i když jde v podstatě o jejich pouhé kopírování do zařízení NAS. Nejsou následně převáděna na jiný druh média a bezpečně uschována.

6 Návrh řešení

Cílem této práce je výběr vhodných bezpečnostních opatření a následný návrh podoby příručky bezpečnosti informací. Prvním a nejdůležitějším krokem je tedy provedení analýzy rizik. Ta se skládá z identifikace a ohodnocení firemních aktiv. Následně se analyzují hrozby a zranitelnosti. Podle zjištěných bezpečnostních rizik se vyberou vhodná opatření a navrhne bezpečnostní politika organizace včetně podoby příručky bezpečnosti informací.

6.1 Analýza rizik v podniku

Na základě znalosti informačních systémů a potřeb organizace lze přistoupit k samotné analýze rizik. První fází je volba nejvhodnější strategie analýzy. Z teoretické části je známo několik použitelných možností. Ideálním případem by byla **detailní analýza rizik**, ale vzhledem k finanční a časové náročnosti a faktu, že společnost zatím neuvažuje o certifikaci, bylo potřeba zvolit efektivnější rovnováhu mezi časem a detailností. Pro analýzu rizik informačního systému organizace byl tedy navržen vlastní postup, který využívá některé prvky jak z **neformální analýzy rizik**, tak z detailní. K hodnocení jsou pak využity kvalitativní metody. Metoda vychází z některých doporučení, uvedených v normách ČSN ISO/IEC TR 13335-3 a ČSN ISO/IEC 27005:2006.

6.1.1 Identifikace a ohodnocení firemních aktiv

Ve spolupráci se zástupci vedení organizace byl sestaven seznam aktiv, která by měla být chráněna. Mezi aktiva jsou zařazeny i služby dodavatelů jako je připojení k internetu a webová prezentace společnosti. Dalším krokem bylo jejich ohodnocení.

Při hodnocení aktiv se bere v úvahu především míra závažnosti možných dopadů při porušení důvěrnosti, dostupnosti nebo integrity vybraného aktiva. Čím více by úspěšný útok na dané aktivum ovlivnil další běh systému, tím vyšší hodnota mu náleží. Pro hodnocení byla zvolena stupnice 1-5, kdy jednotlivé úrovně jsou barevně odlišeny. (7)

Stupnice pro hodnocení aktiv:

Zanedbatelný význam	1
Nízký význam	2
Střední význam	3
Vysoký význam	4
Kritické aktivum	5

Význam jednotlivých stupňů při hodnocení aktiv:

1) Aktivum má pro podnik **zanedbatelný význam**. Jeho poškození se neprojeví mimo podnik, nedojte tím k porušení žádných právních norem a vznikne škoda do 50 000kč.
2) **Nízký význam**. Může v malém rozsahu ovlivnit i okolí firmy, ne však úroveň poskytovaných služeb. Může dojít k porušení právních norem s možným finančním postihem do 50 000kč.
3) **Středně významné aktivum**. Promítá se do kvality služeb a může způsobit finanční potíže i poškození dobrého jména firmy. Správní řízení nebo soudní pře s postihem přesahujícím 50 000kč.
4) **Velmi významné aktivum**. Způsobí veřejnou negativní publicitu či trestní stíhání. Jeho poškozením může dojít k vážnému zranění i ohrožení života. Ztráta důvěry obchodních partnerů.
5) **Kritické aktivum**. Jeho poškozením vznikají existenční problémy společnosti. Je potřebné pro zachování kontinuity provozu. Jeho poškozením může dojít i k vážným zraněním skupiny osob a vysokým finančním ztrátám.

Seznam ohodnocených aktiv společnosti:

Skupina	Aktivum	Hodnota
Technické vybavení	Server Linux	4
	Server Windows	4
	HDD serveru	5
	Router	2
	Modem	2
	UPS zdroj	3
	Switche	3
	Kamerový systém	1
	Video server	1
	Tiskárny	1
	Pracovní stanice zaměstnanců	2
	HDD pracovních stanic	3
	Podniková síť	3
	Dataprojektor	1
Programové vybavení	MS Windows Server 2003	4
	Linux Debian	4
	SAP Business One ERP	5
	MS SQL databáze	4
	Operační systémy pracovních stanic	3
	Codewarrior	2
	Autocad	2
	Docházkový systém	3
	Účetní program	2
	Výrobní IS	4
	MS Office	2
Data v el. Podobě	Projekty a plány	5
	Zálohy dat	5
	Rozpracované dokumenty na stanicích	3
	Zdrojové kódy programů	4
	Osobní údaje zaměstnanců	5
Papírové dokumenty	Účetnictví	4
	Smlouvy s dodavateli/odběrateli	3
	Výrobní dokumentace	5
	Licenční smlouvy	3
	Dokumentace projektů	4
Služby	Připojení k internetu	2
	Web společnosti	1
	Elektronická pošta	3
Nemovitý majetek	Budova	4

Tabulka 3: Seznam aktiv. (Vytvořeno pro potřeby DP)

6.1.2 Identifikace a ohodnocení hrozeb

Dalším úkolem je identifikace hrozeb, které nepříznivě působí na aktiva společnosti. Každá z identifikovaných hrozeb se váže k jednomu, nebo více aktivům, ležícím uvnitř stanoveného rozsahu ISMS.

Část hrozeb byla vybrána z katalogu hrozeb, popsaného normou ISO/IEC TR 13335 a standardem BS 7799-3, část potom na základě zkušeností s konkrétními hrozbami v analyzované společnosti. Vhodným nástrojem k výběru hrozeb je také produkt CRAMM.

U každé hrozby je uveden příklad zranitelnosti, který by hrozba mohla zneužít. Následně se ohodnotila pravděpodobnost jejího výskytu na stupnici 1-5 od velmi nepravděpodobného po téměř jistý výskyt.

Konkrétní názvy některých hrozeb byly oproti jejich podobě uvedené v normě upraveny, aby lépe vystihovali danou nepříznivou situaci v analyzované společnosti.

Stupnice pravděpodobnosti výskytu hrozby:

Velmi nepravděpodobný	1
Málo pravděpodobný	2
Středně pravděpodobný	3
Velmi pravděpodobný	4
Téměř jistý	5

Seznam identifikovaných hrozeb s pravděpodobnostmi jejich výskytu (P):

Druh	Hrozba	P	Příklad zranitelnosti
Přírodní	Poškození aktiva vodou / povodní	1	Umístění aktiv do blízkosti vodního potrubí nebo záplavové oblasti
	Poškození zařízení úderem blesku	3	Citlivost zařízení na elektrostatický výboj, citlivost na přepětí/výpadek napájení
	Poškození požárem	1	Umístění aktiv do míst náchylným ke vzniku požáru. Špatná protipožární prevence
	Výpadek elektrického proudu	3	Závada na elektroinstalaci, blesk, spadlé vedení, příliš velký odběr proudu
	Výpadek internetu	3	Závada na přívodní kabeláži, Problém na straně poskytovatele
	Poškození zařízení prachem	4	Citlivost zařízení / média na prach
Úmyslné	Krádež zařízení	3	Nedostatečná kontrola a evidence firemního majetku, nedostatečná fyzická ochrana objektu
	Krádež dokumentů nebo médií	3	Nedostatečná kontrola externích subjektů v budově, zabezpečení dokumentů a výměnných médií
	Vnější útok	2	Nedostatečné zabezpečení firemních aktiv vůči vnějšímu okolí firmy
	Interní sabotáž	2	Nesprávně přidělená přístupová práva zaměstnanců, špatné zabezpečení firemních aktiv
	Počítačový virus	3	neaktualizovaný systém, chybějící antivir, nezodpovědné chování na internetu, přenosná média
	Pomsta bývalého zaměstnance	2	Neodebrání všech přístupových práv po ukončení pracovního poměru
	Nedodržování směrnic a postupů ISMS	3	Špatně ošetřené pracovní smlouvy, neznalost hrozeb, nízké bezpečnostní povědomí
	Podvržená uživ. Identita	3	Nedokonalý systém identifikace, autentizace a autorizace uživatele
	Porušení mlčenlivosti zaměstnance	3	Špatně ošetřené pracovní smlouvy, neznalost hrozeb, nízké bezpečnostní povědomí
	Neoprávněné získání přístupových práv	3	Nízké bezpečnostní povědomí zaměstnanců, špatné ošetření pracovní smlouvy
	Zneužití přístupových oprávnění	3	Chybné přidělení pravomocí
Neúmyslné	Selhání HW	3	Nedostatečná údržba a výměny HW zařízení
	Selhání SW	3	Neodborná instalace, neaktualizovaný SW
	Selhání sítě	4	Neodborná správa, nedostatečná údržba
	Nedostatečné bezpečnostní povědomí zaměstnanců	4	Absence bezpečnostních směrnic a školení v oblasti bezpečnosti informací
	Porucha vzduchotechniky serverovny	2	Nedostatečná údržba, náchylnost na prach, vlhkost
	Únik důvěrných informací	2	Špatné zabezpečení informačních aktiv, nízké bezpečnostní povědomí zaměstnanců
	Chyba uživatele ICT	5	Nedostatečné zkušenosti zaměstnanců, nepozornost

Tabulka 4: Seznam hrozeb. (Vytvořeno pro potřeby DP)

Na základě identifikovaných aktiv a zjištěných hrozeb byla sestavena tzv. **matice zranitelnosti.** V ní se setkávají jednotlivé hrozby s aktivy a jejich vztah je opět ohodnocen na stupnici 1-5. Tato hodnota udává, s jak vysokou pravděpodobností může hrozba způsobit škodu na daném aktivu.

	Poškození vodou	Poškození bleskem	Poškození požárem	Výpadek el. proudu	Výpadek internetu	Poškození prachem	Krádež zařízení	Krádež dokumentů/médií	Vnější útok	Interní sabotáž	Počítačový virus	Pomsta býv. zaměstnance	Nedodržení směrnic a postupů	Podvržená uživ. identita	Porušení mlčenlivosti zam.	Neop. získání přís. práv	Zneužití přístup. oprávnění	Selhání HW	Selhání SW	Selhání sítě	Nedost. bezp. povědomí zam.	Por. vzduchotech. serverovny	Únik důvěrných informací	Chyba uživatele ICT
Server Linux	2	3	3	2	3	3	2		4	4		3	2					5			4	5		3
Server Windows	2	3	3	2		3	2		1	4			2					5			4	5		2
HDD serveru	3	3	3	2		3	4			5			3					5			5	5		
Router	2	3	3	3		2	1		4	3			1					2		4	2	2		3
Modem	2	3	3	3		2	1			3			1					2		3	2	2		
UPS zdroj	3	2	3			1	1			2			1					4			3			
Switche	2	3	3	3		2	1			3			1					3		3	2	2		2
Kamerový systém	3	3	2	3	2	2	1		4	3		4	1					5			3	1		
Video server	2	3	3	3		2	1			3			1					2			1	2		
Tiskárny	1	2	2	3		3	1			2			1					3						
Pracovní stanice zaměstnanců	2	3	2	3		2	2		2	4		3	2					3			3			3
HDD pracovních stanic	3	3	2	3		2	3		2	4			3					4			4			
Podniková síť	2	2	3	3	2					4			2					4			3			2
Dataprojektor	1	1	1	3		4	3			2								3						
MS Windows Server 2003											5		4	4		4	3		5		2			2
Linux Debian											3		4	4		4	3		3		2			3
SAP Business One ERP													4	5		5	4		4		3			4
MS SQL databáze											3		4	4		4	3		5		3			4
Operační systémy prac. stanic											5		3	3		3	2		5		2			3
Codewarrior																			1					1
Autocad																			2					2
Docházkový systém												4	1	2		2	1		4		2			3
Účetní program											2		1						4		1			3
Výrobní IS													3	2		2	1		5		2			4
MS Office											2								2					1
Projekty a plány			3					4		4	2		2	4	3	4	3				3		5	2
Zálohy dat	3	3	4	2		3	5	5		4	3		5	3		3	2			3	5			4
Rozpracované dokumenty na pc			2	4				4		4	5		4	3	2	3	2				4		3	5
Zdrojové kódy programů			2	2				4		4	3		3		3						4		4	5
Osobní údaje zaměstnanců								5		5	4		4		4						4		5	3
Účetnictví	2		2					4		3			3		4						2		4	
Smlouvy s dodavateli/odběratel	2		2					4		3			2		3						2		3	
Výrobní dokumentace	2		2					4		3			3		2						3		2	
Licenční smlouvy	2		2					4		3			2		1						2		1	
Dokumentace projektů	2		2					4		3			3		5						3		5	
Připojení k internetu									2		3							2						
Web společnosti												3				3	3							
Elektronická pošta									2	3	4	3	3						3	4	3			2
Budova	4	2	4							2		3												

Tabulka 5: Matice zranitelnosti. (Vytvořeno pro potřeby DP)

6.1.3 Výpočet míry rizika

Posledním krokem je výpočet míry rizika pro každou kombinaci hrozba – aktivum. Toto riziko je vypočítáno tří faktorovou metodou, podle vzorce: R = A × H × Z, kde R je míra rizika, A hodnota aktiva, H pravděpodobnost hrozby a Z zranitelnost. (5)

		Poškození vodou	Poškození bleskem	Poškození požárem	Výpadek el. proudu	Výpadek internetu	Poškození prachem	Krádež zařízení	Krádež dokumentů/médií	Vnější útok	Interní sabotáž	Počítačový virus	Pomsta býv. zaměstnance	Nedodržení směrnic a postupů	Podvržená uživ. Identita	Porušení mlčenlivosti zam.	Neop. získání přís. práv	Zneužití přístup. oprávnění	Selhání HW	Selhání SW	Selhání sítě	Nedost. bezp. povědomí zam.	Por. vzduchotech. serverovny	Únik důvěrných informací	Chyba uživatele ICT	
		1	3	1	3	3	4	3	3	2	2	3	2	3	3	3	3	3	3	3	4	4	2	2	5	max
Server Linux	4	8	36	12	24	36	48	24	0	32	32	0	24	24	0	0	0	0	60	0	0	64	40	0	60	64
Server Windows	4	8	36	12	24	0	48	24	0	8	32	0	0	24	0	0	0	0	60	0	0	64	40	0	40	64
HDD serveru	5	15	45	15	30	0	60	60	0	0	50	0	0	45	0	0	0	0	75	0	0	100	50	0	0	100
Router	2	4	18	6	18	0	16	6	0	16	12	0	0	6	0	0	0	0	12	0	32	16	8	0	30	32
Modem	2	4	18	6	18	0	16	6	0	0	12	0	0	6	0	0	0	0	12	0	24	16	8	0	0	24
UPS zdroj	3	9	18	9	0	0	12	9	0	0	12	0	0	9	0	0	0	0	36	0	0	36	0	0	0	36
Switche	3	6	27	9	27	0	24	9	0	0	18	0	0	9	0	0	0	0	27	0	36	24	12	0	30	36
Kamerový systém	1	3	9	2	9	6	8	3	0	8	6	0	8	3	0	0	0	0	15	0	0	12	2	0	0	15
Video server	1	2	9	3	9	0	8	3	0	0	6	0	0	3	0	0	0	0	6	0	0	4	4	0	0	9
Tiskárny	1	1	6	2	9	0	12	3	0	0	4	0	0	3	0	0	0	0	9	0	0	0	0	0	0	12
Pracovní stanice zaměstnanců	2	4	18	4	18	0	16	12	0	8	16	0	12	12	0	0	0	0	18	0	0	24	0	0	30	30
HDD pracovních stanic	3	9	27	6	27	0	24	27	0	12	24	0	0	27	0	0	0	0	36	0	0	48	0	0	0	48
Podniková síť	3	6	18	9	27	18	0	0	0	0	24	0	0	18	0	0	0	0	36	0	0	36	0	0	30	36
Dataprojektor	1	1	3	1	9	0	16	9	0	0	4	0	0	0	0	0	0	0	9	0	0	0	0	0	0	16
MS Windows Server 2003	4	0	0	0	0	0	0	0	0	0	0	60	0	48	48	0	48	36	0	60	0	32	0	0	40	60
Linux Debian	4	0	0	0	0	0	0	0	0	0	0	36	0	48	48	0	48	36	0	36	0	32	0	0	60	60
SAP Business One ERP	5	0	0	0	0	0	0	0	0	0	0	0	0	60	75	0	75	60	0	60	0	60	0	0	100	100
MS SQL databáze	4	0	0	0	0	0	0	0	0	0	0	36	0	48	48	0	48	36	0	60	0	48	0	0	80	80
Operační systémy prac. stanic	3	0	0	0	0	0	0	0	0	0	0	45	0	27	27	0	27	18	0	45	0	24	0	0	45	45
Codewarrior	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	10	10
Autocad	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	20	20
Docházkový systém	3	0	0	0	0	0	0	0	0	0	0	0	24	9	18	0	18	9	0	36	0	24	0	0	45	45
Účetní program	2	0	0	0	0	0	0	0	0	0	0	12	0	6	0	0	0	0	0	24	0	8	0	0	30	30
Výrobní IS	4	0	0	0	0	0	0	0	0	0	0	0	0	36	24	0	24	12	0	60	0	32	0	0	80	80
MS Office	2	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	12	0	0	0	0	10	12
Projekty a plány	5	0	0	15	0	0	0	0	60	0	40	30	0	30	60	45	60	45	0	0	0	60	0	50	50	60
Zálohy dat	5	15	45	20	30	0	60	75	75	0	40	45	0	75	45	0	45	30	0	0	60	100	0	0	100	100
Rozpracované dokumenty na pc	3	0	0	6	36	0	0	0	36	0	24	45	0	36	27	18	27	18	0	0	0	48	0	18	75	75
Zdrojové kódy programů	4	0	0	8	24	0	0	0	48	0	32	36	0	36	0	36	0	0	0	0	0	64	0	32	100	100
Osobní údaje zaměstnanců	5	0	0	0	0	0	0	0	75	0	50	60	0	60	0	60	0	0	0	0	0	80	0	50	75	80
Účetnictví	4	8	0	8	0	0	0	0	48	0	24	0	0	36	0	48	0	0	0	0	0	32	0	32	0	48
Smlouvy s dodavateli/odběrateli	3	6	0	6	0	0	0	0	36	0	18	0	0	18	0	27	0	0	0	0	0	24	0	18	0	36
Výrobní dokumentace	5	10	0	10	0	0	0	0	60	0	30	0	0	45	0	30	0	0	0	0	0	60	0	20	0	60
Licenční smlouvy	3	6	0	6	0	0	0	0	36	0	18	0	0	18	0	9	0	0	0	0	0	24	0	6	0	36
Dokumentace projektů	4	8	0	8	0	0	0	0	48	0	24	0	0	36	0	60	0	0	0	0	0	48	0	40	0	60
Připojení k Internetu	2	0	0	0	0	0	0	0	0	8	0	18	0	0	0	0	0	0	12	0	0	0	0	0	0	18
Web společnosti	1	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	9	9	0	0	0	0	0	0	0	9
Elektronická pošta	3	0	0	0	0	0	0	0	0	12	18	36	18	27	0	0	0	0	0	27	48	36	0	0	30	48
Budova	4	16	24	16	0	0	0	0	0	0	16	0	24	0	0	0	0	0	0	0	0	0	0	0	0	24
	max	16	45	20	36	36	60	75	75	32	50	60	24	75	75	60	75	60	75	60	60	100	50	50	100	

Tabulka 6: Matice rizik. (Vytvořeno pro potřeby DP)

Pro lepší práci se zjištěnými hodnotami rizik jsem tyto rozdělil do tří kategorií na **nízké**, **střední** a **vysoké** riziko. Zvolil jsem hrubější tří stupňovou stupnici, oproti čtyř stupňové, která byla popsána v teoretické části. Nepracuji tedy s pojmem kritické riziko. Teoreticky by při použité tří faktorové metodě mohlo riziko nabývat hodnoty až 125, při maximálním ohodnocení aktiva [5], nejvyšší pravděpodobnosti výskytu hrozby [5] a nejvyšší zranitelnosti [5]. Tam kde jsou v matici rizik nulové hodnoty, riziko není. Kategorie rizik jsem tedy rozdělil tímto způsobem:

1– 40	**Nízké** riziko
41 – 80	**Střední** riziko
81 – 125	**Vysoké** riziko

Rizika s nízkou hodnotou je obvykle možné přijmout, jelikož opatření, která by tato rizika dále snížila, svými náklady snadno přesáhnout možné škody, ke kterým rizika vedou. Jde o jevy, které s malou pravděpodobností vedou k nízkému dopadu na činnost podniku. I když pořizovací ceny aktiv mohou být relativně vysoké (pracovní stanice zaměstnanců, router, dataprojektor apod.), jejich náhrada může být okamžitá, a tak ztráty při jejich výpadku budou minimální.

U středně vysokých rizik již může snadno dojít k ovlivnění činnosti podniku nebo oddělení. Tato rizika je proto potřeba snižovat účinnými opatřeními na přijatelnou úroveň.

Vysoká rizika pak vedou k velmi vážným dopadům na celý podnik a je nutné je redukovat s nejvyšší prioritou.

Z provedené analýzy rizik vyplynulo, že podnik ohrožují:

- 5 Vysokých rizik
- 81 Středních rizik
- 262 Nízkých rizik

6.2 Výběr opatření

Opatření pro snížení rizik v oblasti bezpečnosti informací byla vybrána podle normy ČSN ISO/IEC 27001, konkrétně podle její přílohy A (1). Přehled všech oblastí, které norma pokrývá, byl uveden v kapitole 4.8. V této kapitole pak konkrétně popisuji jednotlivá opatření, vybraná na základě výsledků analýzy rizik. Vzhledem k faktu, že společnost prozatím neusiluje o získání certifikátu ISO 27001, věnuje se tato práce jen zavedení nejdůležitějších (pro analyzovanou společnost) z celkových 139 opatření, které norma definuje. Návrhy řešení jednotlivých opatření vycházejí z normy ISO 27002, což je soubor nejlepších praktik při zavádění ISMS v organizaci, a literatury (7).

6.2.1 Oblast A.5: Bezpečnostní politika informací

Opatření **A.5.1.1** - **Dokument bezpečnostní politiky informací**

Vytvoření dokumentu bezpečnostní politiky informací (viz kapitola 4.5). Tento dokument musí schválit vedení podniku a také s ním prokazatelně seznámit všechny zaměstnance a případné externí dodavatele či odběratele.

Dokument by měl obsahovat:

- Cíle a definovaný význam bezpečnosti informací pro společnost.
- Definice základních bezpečnostních zásad a principů.
- Určení odpovědností a pravomocí souvisejících s bezpečností informací.
- Vyjádření zájmu v dalším rozvoji a prohlubování bezpečnosti informací.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Vytvoření dokumentu bezpečnostní politiky 30 hodin.
Zveřejnění politiky a seznámení zaměstnanců 4 hodiny.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Vedení společnosti

Opatření **A.5.1.2 - <u>Přezkoumání bezpečnostní politiky informací</u>**

Cílem tohoto opatření je zajistit pravidelnou revizi bezpečnostní politiky organizace. Tímto úkolem by měl být pověřen vlastník bezpečnostní politiky. V pravidelném intervalu (vhodný interval přezkoumání by u analyzované společnosti mohl být 1 rok, nebo při významné změně či objevení závažné hrozby) je potřeba posoudit příležitosti ke zlepšení organizace bezpečnosti informací a přizpůsobit pravidla současným potřebám podniku.

Potřebné zdroje pro přijmutí opatření (v plánovaných intervalech):

Finanční: Žádné.

Časové: Přezkoumání a upravení bezpečnostní politiky 20 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

6.2.2 Oblast A.6: Organizace bezpečnosti informací

Opatření **A.6.1.1** - **<u>Závazek vedení směrem k bezpečnosti informací</u>**

Vedení organizace dává tímto závazkem najevo svou vůli zajistit podporu (včetně finančních zdrojů) prosazení bezpečnosti informací v podniku. To znamená, že i vedení je povinno se všemi platnými pravidly řídit a jasně tak ukazovat celé organizaci, že bezpečnost informací je důležitou součástí firemní kultury. Tento závazek je uveden v bezpečnostní politice podniku.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Formulace závazku vedení směrem k bezpečnosti informací 10 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Vedení společnosti

Opatření **A.6.1.3 - <u>Přidělení odpovědností v oblasti bezpečnosti informací</u>**

Musí být jasně definovány odpovědnosti, role a pravomoci spojené s řízením bezpečnosti informací. Je potřeba identifikovat dílčí aktivity i odpovědnosti a pravomoci účastníků zanést do směrnic. Vedoucí jednotlivých oddělení se stávají prostředníky a jsou spoluodpovědní za vzájemnou koordinaci při řešení bezpečnostních incidentů. Podřízení pracovníci hlásí problém svému vedoucímu oddělení a ten pak předává zjištěné skutečnosti bezpečnostnímu manažerovi, který zabezpečí vyřešení bezpečnostního incidentu. Všechny skutečnosti musí být dokumentovány a zaměstnanci musí být seznámeni s těmito postupy. Vedoucí pracovníci mohou jednotlivé úkoly dále delegovat na své podřízené, ale sami za ně odpovídají.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Definovat role a odpovědnosti jednotlivých vedoucích pracovníků 8 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.6.2.1 - <u>Identifikace rizik plynoucích z přístupu externích subjektů</u>**

Před tím, než je externím subjektům umožněn přístupu k informacím a informačním aktivům podniku, je nutno provést bezpečnostní analýzu a identifikaci rizik plynoucích z tohoto přístupu. Předmětem analýzy je technické vybavení a způsob připojení. Na základě posudku a po odstranění případných zjištěných nedostatků, je externímu subjektu umožněno připojení do firemní sítě a jejího využívání. Toto opatření se týká především externích pracovníků vývoje, kteří přistupují do firemní sítě prostřednictvím Wi–Fi přístupového bodu. Opatření se vztahuje také na fyzický přístup externích pracovníků, nebo dodavatelů služeb do jednotlivých kanceláří nebo serverovny, kde je nutno stanovit nejpřísnější opatření.

Potřebné zdroje pro přijmutí opatření (pro jeden externí přístup):

Finanční: Žádné.

Časové: Posouzení vhodnosti připojení externího subjektu 2 hodiny.
Analýza rizik přístupu externího subjektu 2 hodiny.
Měsíční kontrola logů serveru a vyhodnocení dodržování pravidel 1 hodina.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Správce IT

Opatření **A.6.2.3 - <u>Bezpečností požadavky v dohodách se třetí stranou</u>**

S každým externím subjektem je nutno sepsat smlouvu o podmínkách přístupu do podnikové sítě. Smlouva obsahuje klausule o neposkytnutí informací třetím stranám, síle používaných hesel, zásady uzamykání počítačů bez dozoru, používání aktualizovaného systému a antivirového programu. Ve smlouvě jsou stanoveny také sankce za porušení ustanovení smlouvy. Smlouva musí pokrývat veškeré relevantní bezpečnostní požadavky. Kromě přístupu do sítě se týkají i správy prostředků pro zpracování informací, nebo dodávky produktů a služeb.

Potřebné zdroje pro přijmutí opatření (pro jeden externí subjekt a činnost):

Finanční: Žádné.

Časové: Vypracování smlouvy o podmínkách přístupu k prostředkům 2 hodiny.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Výkonný ředitel

6.2.3 Oblast A.7: Řízení aktiv

Opatření **A.7.1.1 - <u>Evidence aktiv</u>**

Toto opatření vyžaduje identifikaci důležitých informačních aktiv podniku a jejich zaevidování, včetně následné pravidelné aktualizace seznamu. Aktiva již byla identifikována v kapitole 6.1.1 – analýza rizik. Aktiva podniku se v čase mění, takže je potřeba stanovit vhodný interval jejich revize. Navrhuji interval 1 rok, nebo při významné změně informačních aktiv (změna informačního systému, nákup serveru, obnova ICT vybavení apod.).

Potřebné zdroje pro přijmutí opatření (v plánovaných intervalech):

Finanční: Žádné.

Časové: Revize informačních aktiv podniku 4 hodiny.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Správce IT

Opatření **A.7.1.2 - Vlastnictví aktiv**

Přiřazení vlastníka ke každému identifikovanému aktivu. Tento vlastník za aktivum odpovídá. Vhodné je stanovit vlastníkem vedoucího oddělení, pod kterého dané aktivum spadá. O tomto přidělení odpovědnosti aktiva je třeba průkazně jeho vlastníka informovat a případné změny vlastníků zaznamenat. Nedílnou součástí tohoto opatření je stanovení revize přidělení aktiv. Zde navrhuji stejný interval jako u opatření A.7.1.1, tedy 1 rok, případně revidovat přidělení v závislosti na personálních změnách ve společnosti.

Potřebné zdroje pro přijmutí opatření (v plánovaných intervalech):

Finanční: Žádné.

Časové: Přiřazení nebo revize vlastníků informačních aktiv 3 hodiny.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.7.1.3 - Přípustné použití aktiv**

Je potřeba určit pravidla pro aktiva, respektive skupiny aktiv, ohledně jejich bezpečného používání. Toto opatření se týká využívání informací i technických prostředků podniku. Například, že data obsahující obchodní tajemství není možné ukládat na výměnná média a notebooky, nebo je v nezašifrované podobě přenášet po síti. Je také potřeba sestavit množinu používaných a povolených aplikací na pracovních stanicích a nastavit odpovědnost jednotlivých pracovníků za obsah pracovních stanic. O všech těchto pravidlech musí být vedena dokumentace a všichni pracovníci musí být s těmito pravidly prokazatelným způsobem seznámeni. Tato pravidla by měla zakázat kopírování, přenášení, tisk či jiné operace, které nejsou přímo spojeny s pracovními povinnostmi, čímž sníží riziko neoprávněného vynesení dat z podniku.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Vytvoření pravidel pro skupiny aktiv a jejich uživatele 20 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

6.2.4 Oblast A.8: Bezpečnost lidských zdrojů

Opatření **A.8.2.2** – **Informovanost a vzděláváni v oblasti bezpečnosti informací**

Na základě tohoto opatření absolvuje každý zaměstnanec společnosti, který při své práci využívá firemní výpočetní techniku, školení o používání výpočetní techniky, firemního programového vybavení, informační bezpečnosti a bezpečnostních rizicích, která hrozí při používání výpočetní techniky. Toto školení by se mělo opakovat jednou ročně. Cílem tohoto opatření je prohlubování bezpečnostního povědomí formou školení, seminářů či jiných vzdělávacích aktivit. Snahou je promítnout definovaná pravidla so skutečného chování všech pracovníků.

Potřebné zdroje pro přijmutí opatření (na jednoho z dvaceti zaměstnanců):

Finanční: Absolvování školení 3 000 Kč.

Časové: Doba strávená cestou a účastí na školení 6 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Personální oddělení

Opatření **A.8.3.2** – **Navrácení zapůjčených prostředků**

Při ukončení pracovního vztahu, smluvního vztahu nebo dohody, musí zaměstnanci, pracovníci smluvních a třetích stran odevzdat veškeré jim svěřené prostředky, které jsou majetkem organizace. Opatření se tedy týká navrácení služebních telefonů, notebooků, klíčů a výměnných médií. Každé z těchto aktiv by mělo být v podniku evidováno a vybaveno číslem. Zde však nastává problém jak zajistit vymazání dat (které jsou majetkem společnosti) na soukromých prostředcích pracovníka, jako jsou flash disky. Proto navrhuji upravit směrnicí zákaz používání soukromých médií a prostředků uvnitř firmy.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Úprava směrnic firmy, zakazující používání vlastních médií 4 hodiny.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.8.3.3** – **Odebrání přístupových práv**

Při ukončení pracovního vztahu, smluvního vztahu nebo dohody, musí být zaměstnancům, pracovníkům smluvních a třetích stran odebrána přístupová práva k jakýmkoliv aktivům a prostředkům firmy. To obnáší uzamčení, nebo úplné smazání přístupových účtů. Toto opatření je pokryto opatřeními v oblasti A.11 – Řízení přístupu.

Potřebné zdroje pro přijmutí opatření:

Řešeno opatřeními a zdroji definovanými v oblasti A.11.

6.2.5 Oblast A.9: Fyzická bezpečnost a bezpečnost prostředí

Opatření **A.9.1.1** - **Fyzický bezpečnostní perimetr**

Pro ochranu prostor, ve kterých se nacházejí informace, nebo prostředky zpracování informací, musí být vytvořeny a používány bezpečnostní perimetry. Ty jsou definovány zdmi, ploty, mřížemi, elektronickým zabezpečovacím systémem apod. Toto opatření je v podniku již zavedeno, ale bylo by vhodné ho revidovat a dále propracovat. Za vnější perimetr je možné považovat pozemek, který je oplocen, vybaven bránou a kamerovým systémem. Dalším perimetrem je samotná budova se zabezpečeným hlavním vchodem, vybavena elektronickým zabezpečovacím systémem. Jako samostatný perimetr je možno považovat i druhé nadzemní podlaží, na které je zaměřena celá práce. Bylo by ale vhodné tento prostor dále rozdělit na několik zabezpečených oblastí. Jednotlivé perimetry pak doplnit přístupovými zařízeními na bázi RFID čipu, které by umožňovalo sledování a omezení přístupu vybraným skupinám zaměstnanců. Tímto opatřením by bylo dosaženo omezení přístupů nepovolaných osob do jednotlivých prostor. Důraz na zabezpečení je třeba věnovat zejména serverovně, kterou je nutné tímto systémem vybavit co nejdříve. V případě bezpečnostního incidentu by bylo zřejmé, který zaměstnanec se v kritickou dobu pohyboval v serverovně, v archivu dokumentů apod. Částečně by toto opatření zabránilo půjčování klíčů od serverovny nepovolaným osobám.

Potřebné zdroje pro přijmutí opatření:

Finanční: Vybavení jednotlivých perimetrů přístupovými body (4 x) 6 000 Kč.

Časové: Rozdělení a zdokumentování perimetrů 10 hodin.

Konfigurace docházkového systému pro nové perimetry 20 hodin.

Monitorování přístupů do perimetrů 4 hodiny měsíčně.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Správce budovy

Opatření **A.9.1.2** - **Fyzické kontroly vstupu osob**

Aby bylo zajištěno, že je přístup do zabezpečených oblastí umožněn pouze oprávněným osobám, musí být tyto prostory chráněny systémem vstupních kontrol. V rámci firmy by byl tento bod pokryt předchozím opatřením A.9.1.1, pomocí přístupových čipů zaměstnanců a uzamykání místností jednotlivých perimetrů. Vzhledem k přístupu osob z vnějšku je toto opatření již ve firmě částečně zavedeno. U vchodu do budovy je nainstalován kamerový systém, a u vstupu do druhého patra je recepce s výhledem na přístupové schodiště. Obsluha recepce však již nevidí na druhou stranu, tedy do chodby mezi jednotlivými kancelářemi. Zde by bylo vhodné umístění kamery, která by tuto chodbu monitorovala a vypracování směrnice pro zaznamenání příchozí osoby, včetně času a účelu návštěvy. Při odchodu pak opět zaznamenat čas odchodu. Musí být zajištěno, aby se osoba návštěvy nemohla sama pohybovat po prostorách firmy. Návštěvní kniha, obsahující předchozí údaje, musí být umístěna na recepci, také je třeba viditelně na recepci vyvěsit pokyny pro chování návštěv v podniku. Tyto pravidla upozorní návštěvy na zákaz volného pohybu a směrnici pro připojení do vyhrazené bezdrátové sítě pro návštěvy.

Potřebné zdroje pro přijmutí opatření:

Finanční: Instalace bezpečnostní kamery a připojení k video serveru 7 000 Kč.

Časové: Stanovení a dokumentace pravidel pro pohyb návštěv 7 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Správce budovy
- Správce IT

Opatření **A.9.1.3** - **Zabezpečení kanceláří, místností a prostředků**

Pro fyzické zabezpečení místností a prostředků, ve kterých se nacházejí zvláště citlivé informace. Toto opatření se tedy týká zejména personálního oddělení a archivu obsahující důvěrné osobní informace zaměstnanců spadající pod zákon na ochranu osobních údajů (4). Tyto místnosti je nutné bezpodmínečně zajistit při každém odchodu. Počítače obsahující důvěrné informace je vhodné připevnit pomocí zámků k pevným konzolím stolů a ochránit je tak proti krádeži. Další důležitou oblastí je serverovna. Přístup do serverovny je již ošetřen opatřeními A.9.1.1 a A.9.1.2. Nutným krokem je ale výměna zámku serverovny za jiný, bezpečnostní, a to z důvodu, že v současné době je v serverovně zámek stejného typu jako v ostatních kancelářích v budově. K těmto zámkům existuje univerzální klíč, který má k dispozici úklidová firma. To s sebou nese ale velmi vysoké riziko. Samostatný přístup uklízečky (nebo kohokoliv, kdo se ke klíči dostane) do serverovny je naprosto vyloučen. V serverovně by tato osoba neměla provádět úklid, protože hrozí polití zařízení vodou, zakopnutí o kabeláž a další hrozby, které by podniku způsobily vysoké škody, nehledě na možnou krádež diskového pole serveru nebo sabotáž. Úklid v serverovně (především jde o prach uvnitř serverového racku) by bylo vhodnější svěřit kompetentní osobě, nejlépe majiteli aktiva, tedy IT správci.

Potřebné zdroje pro přijmutí opatření:

Finanční: Bezpečnostní zámek a sada označených klíčů 800 Kč.
Zámky počítačů (5x) 500 Kč.

Časové: Montáž bezpečnostních prvků 4 hodiny.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.9.2.1** - **Umístění zařízení a jeho ochrana**

Cílem je zajištění bezpečnosti zařízení. Omezení fyzického přístupu je součástí předchozích opatření oblasti A.9. Další rizika, která je potřeba snižovat plynou z hrozeb prostředí, ve kterém se zařízení vyskytují. Je nutné umisťovat zařízení tak, aby byla zachována jejich fyzická bezpečnost a byly zachovány bezpečné provozní podmínky. Toto opatření by bylo vhodné prosadit hlavně v serverovně. Bezpečné provozní podmínky zajišťuje vzduchotechnika, která dodává do serverovny čerstvý vzduch, potřebný k chlazení aktivních prvků. Veškeré aktivní prvky by bylo vhodné umisťovat z důvodu ochrany proti zatopení do výšky minimálně 30 cm. Serverový rack by měl být dostatečně prostorný kvůli odvodu tepla

z jednotlivých zařízení. Stávající rack (velikost 24U) je plně obsazen, proto navrhuji zakoupení nového, prostornějšího racku. Byl zvolen 19" rack 42U o rozměrech 2020 x 800 x 1000 mm od firmy Digitus. Dostatečně prostorný rack umožní lepší organizaci kabeláže a chlazení.

Potřebné zdroje pro přijmutí opatření:

Finanční: Rack Digitus Server-Line 42U 19" 17 000 Kč.

Časové: Instalace síťových prvků do racku 8 hodin.

Za zavedení odpovídá:

- Správce IT

Opatření **A.9.2.2** - **Podpůrná zařízení**

Zařízení by měla být chráněna před výpadkem elektrického proudu a selháním dalších podpůrných prvků. Vybavení všech pracovních stanic zaměstnanců záložními napájecími zdroji by bylo velmi nákladné a převýšilo by náklady spojené tímto rizikem. Proto jsou jimi vybaveny pouze počítače v ekonomickém oddělení a účtárně, kde se provádějí kritické operace v informačním systému SAP. Další záložní napájecí zdroj se nachází v serverovně a chrání před výpadkem napájení serverový rack se servery a aktivními prvky. Tento zdroj byl ale shledán jako zastaralý a nedostatečný. Navíc není propojen datovou sběrnicí se serverem, takže neumožňuje automatické bezpečné vypnutí. Navrhuji zakoupení nového, lépe vybaveného a dimenzovaného záložního zdroje, a připojit jej k serverům. Stávající zdroj by mohl zůstat pouze pro napájení ostatních aktivních prvků, jako jsou switche a routery.

Další bezpečnostní hrozbu představuje pojistková skříň, umístěna na chodbě, která není chráněna proti manipulaci nepovolanými osobami. Jističe v této skříni chrání jak veškeré kanceláře, tak i serverovnu. Kdokoliv, kdo jde po chodbě, může tedy během několika vteřin odpojit od napájení kompletní ICT vybavení firmy. Je bezpodmínečně nutné vybavit tuto skříň zámkem a klíč přidělit pouze kompetentním zaměstnancům jako je správce budovy a IT správce.

Důležitým podpůrným zařízením je vzduchotechnika serverovny. Protože se jedná o relativně malou místnost bez oken, je v letních měsících tato technika nezbytná pro odvedení tepelného výkonu všech zařízení mimo místnost serverovny. Její výpadek by měl katastrofální následky a během několika hodin by mohlo dojít k vážnému poškození vybavení nebo vzniku požáru. Serverovna je vybavena detektorem požáru a ten je napojen na pult centrální ochrany smluvní bezpečnostní agentury. Doporučuji tímto způsobem

monitorovat i funkci vzduchotechniky. Nejlépe teplotním čidlem, které by při překročení jisté meze vyhlásilo poplach. Bezpečnostní agentura poté upozorní na mobilní telefony majitele firmy a správce budovy.

Vnější přípojka k internetu musí být vybavena přepěťovou ochranou.

Potřebné zdroje pro přijmutí opatření:

Finanční: Zdroj Dell UPS, Tower, 1000W, usb propojení se serverem 9 000 Kč.
Uzamykatelná pojistková skříň 3 000 Kč.
Teplotní čidlo a jeho připojení k zabezpečovacímu systému 2 200 Kč
Přepěťová ochrana 500 Kč

Časové: Instalace UPS zdroje 3 hodiny.
Montáž pojistkové skříně 5 hodin.
Montáž bezpečnostních prvků 5 hodin.

Za zavedení odpovídá:

- Správce IT

Opatření **A.9.2.4 - <u>Údržba zařízení</u>**

V podniku je potřeba zavést plán pravidelných revizí a údržby všech zařízení v rámci rozsahu ISMS pro prohloubení jejich spolehlivosti a dlouhodobé funkčnosti. Musí být stanoven kompetentní zaměstnanec, který bude odpovědný za fyzické provádění kontrol a revizí používaných zařízení. O revizích je nutno vést záznamy a upozorňovat na nalezené nedostatky. Součástí těchto revizí by mělo být i čištění pracovních stanic nebo serverů od prachu. Důležité je i pravidelné testování funkce záložních napájecích zdrojů a vzduchotechniky serverovny. Dalšími činnostmi pak může být kontrola a doplnění toneru v tiskárnách, nebo výměna výbojky v projektoru. Přijatelný interval kontroly a údržby by byl jeden měsíc.

Potřebné zdroje pro přijmutí opatření (v plánovaných intervalech):

Finanční: Žádné.

Časové: Sestavení plánu revize a údržby zařízení 8 hodin.
Pravidelná kontrola a údržba zařízení 10 hodin

Za zavedení odpovídá:

- Správce IT

6.2.6 Oblast A.10: Řízení komunikací a řízení provozu

Opatření **A.10.5.1** – **Zálohování informací**

Proces zálohování obnáší pravidelné pořizování záložních kopií dat a také jejich následné testování. Týká se všech dat i programového vybavení s cílem zajištění případné obnovy datových zdrojů nebo chodu programového vybavení a systémů.

Je nutné vypracovat a následně dodržovat plán zálohování zvolit správné uložení záložních kopií a také průběžně testovat jejich funkčnost. Podle (10) největší škody při provozování informačního systému souvisejí právě s nevhodnou strategií zálohování dat a jeho nedůsledném provádění. Klíčovým krokem je tedy volba vhodné strategie.

Proces zálohování je v podniku již částečně řešen. Ve skladovací hale je umístěno diskové pole, na které se každý den překopírují soubory z datového serveru. Pro tento proces ale neexistuje žádná závazná směrnice a hlavně se týká pouze dat uložených na serveru. Nezahrnuje programy, systémy a ani data uložená na pracovních stanicích. Z výsledku dotazníku v kapitole 5.5.2, vyplynulo, že pravidelně data na svém počítači zálohuje pouhých 22% zaměstnanců.

Jako první krok navrhuji zavedení adresářové služby Active Directory, nastavení domén a uživatelských účtů pro jednotlivé uživatele. Tento systém výrazně zefektivní správu a zvýší bezpečnostní úroveň. Současně bude tímto krokem pokryto mnoho hrozeb. Uživatelé budou nuceni používat hesla pro přihlášení do domény (heslo nyní používá jen 75% uživatelů), uživatele bude možno rozdělit do skupin a těm poté přiřadit sadu oprávnění a především budou data jejich pracovních adresářů fyzicky umístěna na serveru. Zálohovat pracně data každé pracovní stanice tedy nebude nutné.

Aktuálně nainstalovaný operační systém Windows Server 2003 však tuto službu nepodporuje, proto si zavedení opatření vyžádá instalaci novějšího systému. Po poradě s vedením byl vybrán produkt Microsoft Small Business Server 2011. Součástí této sady produktů je Windows Server 2008 R2 a také SQL Server 2008 R2.

Dalším krokem je zvolit vhodnou strategii zálohování. Záloha tvoří pojistku dat před havárií. Cílem je rychle obnovitelný, plně funkční stav systému po bezpečnostním incidentu. Rozlišujeme tedy archiv, který slouží k uložení dat na bezpečném místě po dlouho dobu (desítky let) a zálohu, kterou můžeme využít ze dne na den, případně s odstupem několika měsíců. Z tohoto rozdělení tedy vyplývají rozdílné požadavky na média pro zálohování a archivaci. Při obnovování dat po havárii jde o čas a každá ztracená minuta může mít vysokou cenu. Je proto nutné vytvořit vhodný plán tvorby a správy záložních kopií. Ty musí být dobře

zabezpečeny před zničením, odcizením a změnou. Proto se ukládají v místnostech k tomu určených. Zásadou je umístění mimo počítač, nejlépe v trezorech nadzemních podlaží budovy. Při skladování těchto médií je potřeba brát v potaz opatření, které se tomuto tématu věnují, konkrétně opatření oblasti A.9: Fyzická bezpečnost a bezpečnost prostředí. Umístění médií do trezoru mimo budovu by ale bylo značně složité a nákladné, protože pouze hlavní budova splňuje požadavky na bezpečnostní perimetr a média by tak byla sice lépe chráněna proti požáru, ale nedostatečně vůči vlivům prostředí a především neoprávněnému přístupu osob. Proto navrhuji jejich umístění do trezoru v kanceláři, která je nejvíce vzdálená od serverovny, na opačné straně budovy. Tím se sníží riziko, že při případném požáru budou zničena jak serverovna, tak uložené média. Pro zálohování postačí disky DVD. Pro archivaci je pak vhodné volit média s delší životností.

Plán zálohování by mohl mít následující podobu:

Pravidelně kopírovat na externí diskové pole přírůstky dat ve dnech pondělí až čtvrtek, vždy po skončení pracovní doby. Každý pátek pak provádět kompletní zálohu včetně vypálení na disky DVD a jejich bezpečné uschování. Zálohy uchovávat na dobu nejméně šesti měsíců. První zálohy z ledna a července každého roku poté archivovat na neomezenou dobu na bezpečném místě mimo pracoviště.

Potřebné zdroje pro přijmutí opatření:

Finanční: Microsoft Small Business Sever 2011 CZ 64bit 15 000 Kč.
Instalace serveru a konfigurace domény 15 000 Kč.

Časové: Vytvoření závazného plánu zálohování 10 hodin.

Za zavedení odpovídá:

- Správce IT
- Manažer bezpečnosti.

Opatření **A.10.7.1** – **<u>Správa výměnných počítačových médií</u>**

Řeší bezpečnost při zacházení s datovými médii. Důležitá je správa těchto zařízení, která zajistí jejich evidenci a sledování předpokládané životnosti zařízení. Po jejím uplynutí zajistí spolehlivou likvidaci. Mezi výměnná média je možno zařadit CD a DVD disky, diskety a flash disky. Každé médium je vhodné vybavit evidenčním číslem a samolepkou. Vhodným opatřením je zákaz vynášení médií mimo budovu firmy, až na výjimky jako jsou služební cesty apod. Evidence médií je důležitá i pro zjištění případné ztráty nebo odcizení. Při

vyřazování starých nebo nepotřebných médií je nutné zajistit jejich fyzickou likvidaci, aby nebylo možné zneužít data v nich obsažená.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Zahrnutí médií do evidence majetku a jejich označení 5 hodin.

Za zavedení odpovídá:

- Správce budovy
- Manažer bezpečnosti

6.2.7 Oblast A.11: Řízení přístupu

Opatření **A.11.1.1** - **Politika řízení přístupu**

Vedení podniku by mělo vytvořit směrnici, která jasně definuje požadavky na bezpečnost přístupu k informacím. Tato směrnice by měla definovat přístupové role pro běžné kategorie činností. Přístupová práva by měla být vázána především na pracovní pozice (role), a ne na konkrétní fyzické osoby. Tento přístup podstatně zjednodušuje správu přístupových práv. Pro vytvoření skupin a definování oprávnění je ideální využít centralizovanou správu operačních systémů, uživatelských účtů a aplikací – Group Policy (skupinová politika), což je funkce serverových operačních systémů společnosti Microsoft. Společnost ale využívá systém Windows Server 2003, který touto funkcí nedisponuje. Opatření A.10.5.1 (zálohování) však zavádí novější systém, Windows Server 2008R2, který již Group Policy plně podporuje. Při řízení přístupu k informacím je nutno respektovat odpovídající legislativní nařízení a ostatní smluvní závazky ve vztahu k ochraně přístupu k datům nebo službám. A pro zvýšení bezpečnosti je vhodné užít pravidlo, že vše co není explicitně dovoleno, je zakázáno. Role udělují svým podřízením vedoucí pracovníci po dohodě s vedením firmy.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Vytvoření směrnice definující přístupové role skupin uživatelů 10 hodin.
Konfigurace Group Policy na serveru 10 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.11.2.1** - **Registrace uživatele**

Zavádí formální postup pro registraci uživatele včetně jeho zrušení, který zajistí přístup uživatele ke všem víceuživatelským systémům a službám. Přičemž každý uživatel by pokud možno měl disponovat svou vlastní, jedinečnou identitou. Sdílení identity vede k nemožnosti jednoznačné prokazatelnosti operací, a tím i následné neschopnosti prosazení individuálních odpovědností jednotlivých osob za provedené operace.

Registrace spočívá v přidělení unikátního přihlašovacího jména, které jasně identifikuje daného uživatele v systému. Přístup k prostředkům a službám mu bude umožněn až po procesu autorizace. Součástí registrace uživatele je také jeho podpis prohlášení, že je seznámen s podmínkami přístupu. Pro zavedení tohoto pravidla je nutné nakoupit dodatečné uživatelské licence pro systém Windows Small Business Server 2011 (který zavedlo opatření A.10.5.1), aby bylo zajištěno, že se každý uživatel přihlásí pod vlastním jménem.

Je vhodné také dodržovat pravidlo, že má-li být se zaměstnancem rozvázán pracovní poměr, nejprve IT oddělení zajistí blokaci všech přístupů a teprve pak se to dotyčnému oznámí. Sníží se tak nebezpečí vynesení dat z organizace, nebo pokusu a pomstu zaměstnavateli.

Důležité také je udržovat záznamy o všech registrovaných uživatelských účtech a jejich oprávněných využívat prostředky a služby.

Potřebné zdroje pro přijmutí opatření:

Finanční: Rozšíření licencí CAL na 15 uživatelů Windows + SQL serverů 22 000 Kč.

Časové: Vytvoření záznamů o uživatelských účtech 10 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.11.2.2** - **Řízení privilegovaného přístupu**

Řídí a omezuje přidělování privilegií uživatelům. Privilegované role jsou například účet „správce“, nebo „administrátor“ s přístupem k funkcím nebo prostředkům, umožňující uživateli možnost překonat systémové nebo aplikační kontroly. Privilegia jsou přidělována jednotlivcům na základě jejich oprávněné potřeby pro použití a jsou samostatně posuzována a schvalována. Je pořízen a zachováván záznam o všech přidělených privilegiích.

Neprivilegovaní zaměstnanci by měli využívat účet s omezenými oprávněními, kde je možno například zabránit instalaci vlastních programů, konfiguraci systému, nebo přístupu k některým službám. Vhodným opatřením je také nastavení synchronizace času na všech

stanicích a zakázání manuálního nastavení. To zabrání případné manipulaci s časovými razítky dokumentů.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Vypracování seznamu privilegovaných uživatelů 2 hodiny.
Konfigurace všech účtů 10 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.11.2.3** - **Správa uživatelských hesel**

Upravuje pravidla pro přidělování a správu hesel k pracovním stanicím, informačnímu systému, nebo elektronické poště. Uživatelé by měli před prvním přihlášením obdržet jedinečné, náhodně vygenerované heslo, které jsou povinni ihned po přihlášení změnit a zvolit vlastní heslo, viz opatření A.11.3.1 o používání hesel. Přidělená jednorázová hesla nesmí být nikde uchována v nechráněné formě. Zaměstnancům jsou předána bezpečným způsobem, ne pomocí elektronické pošty. Uživatelé musí přijetí hesla potvrdit a podepsat prohlášení, že budou hesla udržovat v tajnosti.

U všech zakoupených systémů s dodavateli přednastavenými hesly je nutné tyto hesla ihned změnit.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Vygenerování hesel pro uživatele a předání spolu s prohlášením 8 hodin.
Výměna všech nedostatečně silných a přednastavených hesel zařízení 3 hod.

Za zavedení odpovídá:

- Manažer bezpečnosti
- Správce IT

Opatření **A.11.2.4** - **Přezkoumávání přístupových práv uživatelů**

Přístupová práva uživatelů je potřeba přezkoumávat v pravidelných intervalech, případně při změně pracovní pozice, nebo ukončení pracovního poměru konkrétního zaměstnance. Přezkoumat je nutné jak přístupová práva uživatelů (zavádí opatření A.11.1.1), tak privilegovaná oprávnění (zavádí opatření A.11.2.2). Veškeré změny je nutno zaznamenat. Intervaly přezkoumání by v analyzované společnosti mohly být stanoveny na půl roku.

Potřebné zdroje pro přijmutí opatření (v plánovaných intervalech):

Finanční: Žádné.

Časové: Přezkoumání a revize přístupových práv a privilegií 6 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

Opatření **A.11.3.1** - **Používání hesel**

Nutnost používání hesel přináší do podniku opatření A.10.5.1, které zavádí službu Active Directory. Opatření A.11.3.1 definuje, jak postupovat při výběru a používání hesel. Za volbu dostatečně silného hesla a za jeho případné zneužití zodpovídají uživatelé. Psaní hesel na jakékoliv viditelné místo a jeho sdělování jiným osobám je zakázáno.

Při tvorbě hesla je nutné dodržet následující pravidla:

- Délka 6 -10 znaků.
- Nesmí obsahovat diakritiku.
- Musí obsahovat číslice.
- Snadno se pamatuje, není třeba je zapisovat.
- Nesmí obsahovat slovo vyskytující se ve slovníku.
- Nesmí obsahovat jméno, přezdívku, nebo obecně známý název.
- Nesmí obsahovat rodné číslo, datum narození, telefon nebo SPZ auta.
- Musí být složeno z různých písmen, ne v řadě se vyskytujících na klávesnici.
- Nic z výše uvedeného, napsáno pozpátku, nebo doplněno o číslici.

Dodržení uvedených pravidel a postupů nevyžaduje žádné dodatečné časové, ani finanční náklady. Každý zaměstnanec si sám zvolí heslo.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Žádné.

Za zavedení odpovídá:

- Uživatelé

Opatření **A.11.3.2** - **Neobsluhovaná uživatelská zařízení**

Po ukončení práce je nutné zajistit pracovní stanici proti neoprávněnému přístupu. Toho je možno docílit buď vypnutím, odhlášením, nebo uzamknutím. Pokud zaměstnanec odchází od počítače pouze dočasně, je nutné se od svého uživatelského účtu buď odhlásit, nebo použít

klávesovou zkratku „symbol Windows“ + „L“, čímž dojde k uzamčení relace. Další vhodnou metodou je nastavení spořiče tak, aby po probuzení vyžadoval heslo. Zde je ale potřeba volit dostatečně krátký interval pro spuštění spořiče, aby toto opatření mělo požadovaný efekt. To však může být značně obtěžující při práci.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Žádné.

Za zavedení odpovídá:

- Uživatelé

Opatření **A.11.3.3** - **Zásada prázdného stolu a prázdné obrazovky monitoru**

Každý zaměstnanec by měl dodržovat zásady při práci s citlivými informacemi, důležitými dokumenty, přenosnými médii a jinými nosiči dat. V případě, že se daný dokument nepoužívá, nebo zaměstnanec opouští kancelář, musí být tento bezpečně uschován. Nejlépe uzamčením ve skříni, nebo zásuvce. Stejná pravidla platí i pro poštovní korespondenci.

Každý zaměstnanec má k dispozici uzamykatelnou zásuvku stolu, takže s tímto opatřením nejsou spjaty žádné dodatečné finanční náklady.

Po ukončení tisku důležitých nebo citlivých materiálů je potřeba vymazat paměť tiskárny, aby nemohly být dokumenty nepozorovaně vytisknuty opakovaně.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Žádné.

Za zavedení odpovídá:

- Uživatelé

6.2.8 Oblast A.12: Akvizice, vývoj a údržba inf. systémů

Opatření **A.12.4.1** – **Správa provozního programového vybavení**

Je potřeba zavést postupy pro kontrolu a ochranu instalovaného a provozovaného programového vybavení. Cílem je kontrolovat, jaké programové vybavení je na servery a pracovní stanice instalováno, zda je řádně prověřen jeho dodavatel a zda neobsahuje žádné nežádoucí služby, viry, nebo trojské koně. Důležité je také ověřit, že daná instalace je

v souladu s licenční politikou výrobce a firma tak neriskuje případný soudní spor. Aktualizace operačních systémů a důležitých programů by měl provádět pouze správce IT. Před každým přechodem na novou verzi programu by se měly vzít v úvahu přínosy této změny spolu s bezpečnostní úrovní nové, často nedostatečně prověřené verze. Přechod na novější operační systém by se měl provést až po důkladném rozmyšlení, zda je tato změna nutná, nebo pokud stávající systém nepodporoval některou ze síťových služeb nebo důležitý firemní proces. Nemělo by se přecházet na nové verze jen z důvodu jejich vydání. Nové verze mohou být méně bezpečné, stabilní a pro uživatele méně intuitivní. Interval kontroly instalovaného softwaru byl zvolen jednou za půl roku.

Potřebné zdroje pro přijmutí opatření (v plánovaných intervalech):

Finanční: Žádné.

Časové: Vypracovat plán kontrol a aktualizací programového vybavení 8 hodin.
Kontrola a aktualizace instalovaného sw na stanicích a serverech 10 hodin

Za zavedení odpovídá:

- Správce IT

6.2.9 Oblast A.15: Soulad s požadavky

Opatření **A.15.1.4** - **Ochrana dat a soukromí osobních informací**

Ochrana dat a soukromí musí být zajištěna v souladu s odpovídajícími legislativními požadavky. V České republice tuto oblast reguluje zákon č. 10/2000 Sb. o ochraně osobních údajů, jehož hlavním gestorem je Úřad pro ochranu osobních údajů. Je potřeba stanovit pravidla, jak s těmito informacemi zacházet a předat je zaměstnancům, kteří s nimi přicházejí do styku. Vypracování politiky ochrany dat a soukromí, její předání a vysvětlení individuálních odpovědností zaměstnancům, by měl zajistit manažer bezpečnosti. Politika musí být vypracována v souladu se zákonem č. 10/2000 Sb.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: Vytvoření politiky ochrany dat a soukromí a poučení zaměstnanců 15 hodin.

Za zavedení odpovídá:

- Manažer bezpečnosti

6.2.10 Doplňující opatření

Opatření A.10.5.1, A.9.2.1 a A.9.2.2 zavádějí nový operační systém pro server, prostorný serverový rack a nový záložní napájecí zdroj. Vzhledem ke stáří aktuálního serveru (5 let), jeho nedostatečného výkonu pro běh SQL serveru se systémem SAP Business One a nutnosti kompletní reinstalace a reorganizace serverovny, bylo po poradě s vedením navrhnuto zakoupení nového, výkonnějšího serveru, na který se zakoupený sytém Microsoft Small Business Server 2011 nainstaluje. Kvůli požadavku na maximální dostupnost stroje byla pro jeho dodání zvolena firma DELL, konkrétně server T320. Tato firma dodá také záložní zdroj. Dalším důvodem této volby byla nabídka dodání všech licencí společnosti Microsoft se slevou 10% při jejich zakoupení spolu s novým serverem. Zvolen byl cenově zvýhodněný balík Microsoft Small Business Server 2011 Standard s rozšířením Premium. Balík obsahuje licence jak pro operační systém Windows server 2008 R2, tak pro databázi SQL server 2008 R2, navíc je k dispozici poštovní systém Microsoft Exchange 2010 a další komponenty. Verze Premium obsahuje 2 licence operačního systému a je tedy možné využít i virtualizace, nebo instalace na 2 fyzické servery. Opatření A.10.5.1 zavádí doménové řízení uživatelských účtů a obnáší nákup rozšiřujících licencí pro další uživatele, takzvané CAL pro celkový počet 15 uživatelů.

Přehled potřebných licencí (náklady na ně jsou již započítány v opatřeních):

Operační systém Small Business Server 64bit, obsahuje 5 licencí	15 000 Kč
Rozšíření PREMIUM, s SQL databází, obsahuje 5 licencí pro klienty	22 000 Kč
doplnění licencí Standard o dalších 10 (do počtu 15)	10 000 Kč
doplnění licencí Premium o dalších 10 (do počtu 15)	12 000 Kč
Celkem za licence:	59 000 Kč

Navrhovaný server T320 má tyto parametry:

- Procesor: Intel® Xeon® E5-2430 2.20GHz, 15M Cache.
- Paměť: 24 GB RDIMM, 1333 MHz.
- Disky: 6 disků SAS do RAID10, 300GB, 10K RPM Hard Drive (Hot Plug).
- Řadič disků RAID s 512MB cache.
- Redundantní napájecí zdroje.
- Karta pro vzdálený přístup, s možností konzoly, zapnutí, vypnutí, monitorování.
- Záruka 5 let s garancí opravy v místě do následujícího pracovního dne.
- Optimální hloubka racku pro montáž serveru je 100 cm, jeho výška v racku je 5U.

Cena serveru: 132 000 Kč

6.2.11 Ekonomická rozvaha projektu

V této kapitole budou vyjádřeny veškeré náklady, které zavedení a provoz ISMS obnáší. Jednotlivá opatření si žádají finanční a časové náklady. Oba druhy pak mohou obsahovat jednorázovou a opakující se časově variabilní složku. Jednorázové náklady jsou uplatněny pouze jednou při zavedení opatření, pravidelné náklady jsou přepočítány na jeden měsíc provozu systému. U některých opatření jejich výši určuje počet událostí / incidentů, které v podniku nastanou. V tomto případě byl proveden odhad a výsledné náklady byly přepočítány na měsíc.

Jednorázové náklady:

- Finanční 258 000 Kč.
- Časové 250 hodin.

Pravidelné měsíční náklady:

- Finanční 5 000 Kč.
- Časové 30 hodin.

Časové náklady je potřeba také vyjádřit v penězích. Hodina práce na odpovídající pozici byla ohodnocena na 330 Kč.

Výsledkem jsou jednorázové náklady ve výši 340 500 Kč a měsíční náklady ve výši 15 000 Kč. Na první rok zavádění a provozu ISMS by podnik vynaložil **520 500** Kč. Každý další rok teoreticky pak pouze **180 000** Kč. Protože je ale ISMS neustálý koloběh založený na PDCA cyklu, jisté finanční výdaje na změny a zavádění nových opatření jsou nevyhnutelné.

Celý návrh by bylo možné pro otestování účinnosti doplnit vnějšími a vnitřními **penetračními testy.** Penetrační testy slouží k ověření odolnosti sítě vůči neoprávněnému průniku. Při tomto druhu testování je využíváno metod hackingu a poskytovatel služby se snaží zachytit a přečíst přenášená data a proniknout zvenčí i zevnitř k uloženým citlivým informacím. Úspěšné průniky analyzuje a navrhne opatření, která jim účinně zabrání. Testuje se průnik jak z internetu přes ADSL připojení, tak průnik do firemní Wi-Fi sítě. Při vnitřním testování se na místo dostaví specialista vybavený potřebnými nástroji a provede testování a sběr údajů. Tyto testy jsou velmi přínosné, avšak ceny se pohybují v řádech desetitisíců.

Jako vhodné ověření zabezpečení sítě by mohl být produkt „Rozšířený test +“, který nabízí společnost Agerit s.r.o (14). Tento test je cenově přijatelný a obnáší tyto úkony:

- Skenování portů pro UDP/IP protokol.
- Testování dostupnosti databází z internetu (SQL servery: MS SQL, MySQL, Oracle).
- Přítomnost trojských koní.
- Kontrola portů TCP/IP a UDP/IP (1 – 65535) např. servery WWW, FTP, mail, DNS.
- Kontrola zranitelnosti hesel.
- Test zranitelnosti systému na DoS a DDos útoky (pouze na žádost zákazníka).
- Analýza nastavení a odborná konzultace na místě (v ceně 2 hodiny).

Cena testu i s příjezdem odborníka do firmy by byla cca 4 500 Kč.

Přínosy navrhovaných opatření a ekonomické zhodnocení celého projektu je popsáno v závěru práce, konkrétně v podkapitole 7.1.

6.3 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti je důležitý dokument, který upřesňuje ochranná opatření, která byla pro daný ISMS vybrána na pokrytí bezpečnostních rizik. Tento dokument je součástí povinné dokumentace pro společnosti usilující o certifikaci o shodě svého ISMS s normou ISO/IEC 27001. Obsahuje výčet jednotlivých opatření a jejich cíle, čili pokrytí některého z bezpečnostních rizik. Pohledem do tohoto prohlášení lze snadno vyhodnotit, zda došlo k pokrytí všech identifikovaných rizik. Prohlášení může být doplněno komentářem, který objasní, proč některá opatření aplikována nebyla. O tento dokument se později opírají i auditoři, kteří se potřebují rychle zorientovat v novém, a tedy pro ně obtížně srozumitelném ISMS. (7)

Úkolem vedení je tedy zvážit vybraná opatření s ohledem na finanční a personální náklady a následně přijmout zbytková rizika. Po výběru a revizi ochranných opatření vždy zůstanou nějaká zbytková rizika. Nelze dosáhnout naprosto bezpečného systému. Tato zbytková rizika mohou být buď akceptována, nebo neakceptována. Je věcí nejvyššího managementu, kterému jsou tato zbytková rizika předložena, jak rozhodne. Jakákoliv odpovědnost nenáleží implementačnímu týmu, ale jen a pouze nejvyššímu managementu společnosti. O tomto přijetí by tudíž mělo rozhodovat výhradně vedení společnosti a nikoliv bezpečnostní manažer, nebo IT správce.

Jestliže riziko není akceptováno, probíhá znovu výběr ochranných opatření a odhadování rizik. Je ale šance, že může být přijato dodatečně ochranné opatření, které je příliš nákladné nebo z hlediska bezpečnosti zbytečné. (13)

6.4 Harmonogram zavádění opatření

Jednotlivá bezpečnostní opatření budou v podniku zaváděna průběžně. Jednak kvůli rozložení finančních výdajů, ale také značným časovým nárokům na práci manažera bezpečnosti a dalších pracovníků, které si zavádění některých opatření vyžádá. Důležité je tedy postupovat systematicky a předem rozmyslet důsledky a návaznosti při zavádění nových opatření. Je potřeba se vyvarovat zbytečným nákladům spojeným například s montáží serveru do nevyhovujících prostor a následně přijmout opatření na jeho přemístění.

První etapou, kterou by bylo vhodné dokončit během nejbližších dvou měsíců je tedy zajištění bezpečnostního perimetru a podpůrných zařízení.

Druhou etapou bude připravení podkladů pro nasazení řízení skupinové politiky uživatelů. Rozdělit uživatele do skupin a přidělit jim oprávnění, případně privilegia. Pro uživatele si připravit vygenerovaná hesla. Před přechodem na nový systém by bylo vhodné mít vypracovány veškeré směrnice a dodatky v pracovních smlouvách, aby zavádění a chod nového systému proběhl pokud možno bez bezpečnostních incidentů. Tato etapa by neměla přesáhnout 2 měsíce.

Třetí etapou je reorganizace serverovny a nasazení nového operačního systému. Tato operace si vyžádá i kompletní reinstalaci informačního systému SAP Business One a reorganizaci všech uživatelských účtů. Proto je nutno počítat s jistým omezením chodu firmy až na několik dní. Kompletní nasazení a zaběhnutí nových systémů a účtů by mělo trvat do dvou týdnů.

Čtvrtou etapou by bylo přijetí plánu zálohování, pokud možno ihned po úspěšném provedení předchozího kroku.

Další etapy pak zahrnují průběžné školení a zvyšování bezpečnostního povědomí zaměstnanců a průběžné doplňování směrnic, dokumentů a opatření, která dosud nebyla z časových důvodů přijata. Během jednoho roku by tak měl proběhnout celý ISMS cyklus, včetně vyhodnocení slabých míst a návrhů zlepšení a změn.

6.5 Návrh podoby příručky bezpečnosti informací

O tom, co je příručka bezpečnosti informací a k čemu slouží, pojednává kapitola 2.2.1. V této kapitole bude probrána metodika návrhu podoby této příručky pro analyzovanou společnost. Tento důležitý dokument obsahuje veškeré popisy procesů a postupů při prosazování jednotlivých bezpečnostních opatření a ve své podstatě obsahuje až na výjimky všechny kapitoly této práce. Struktura příručky vychází přímo ze struktury samotné normy ISO/IEC 27001:2005.

Úvodní strana příručky bezpečnosti informací bude obsahovat tabulku pro průběžné zaznamenávání změn. Pokud dojde k nějaké změně, je nutné tuto změnu popsat a zaznamenat číslo změny, změněné stránky, datum a jméno s podpisem autora změny. Další tabulka na úvodní straně slouží k identifikaci autora dokumentu, potvrzení o schválení a případné další revize.

Na **druhé straně** se nachází obsah příručky bezpečnosti, který má následující strukturu:

1. **Předmět normy**
2. **Normativní odkazy**
3. **Termíny a definice**
4. **Systém managementu bezpečnosti informací**
5. **Odpovědnost vedení**
6. **Interní audity ISMS**
7. **Přezkoumání ISMS vedením organizace**
8. **Zlepšování ISMS**

Následují jednotlivé kapitoly:

1. Předmět normy

V této kapitole je popsán účel příručky. Určuje zásady ochrany informací v dané organizaci a zavádí jednoznačný systém odpovědnosti spolu se zajištěním důvěrnosti, integrity a dostupnosti informačních zdrojů. Předmětem je ochrana jakýchkoliv nosičů dat a informací, jako jsou písemné materiály a dokumenty, magnetická média (pevné disky), optická média a další paměťová zařízení. Chráněny musí být také všechny formy přenosu údajů a informací.

V této kapitole by také mělo být uvedeno, pro jakou firmu příručka slouží, a že je závazná pro všechny uživatele informačního systému.

2. Normativní odkazy

Zde je potřeba odkázat na všechny podpůrné normy a dokumenty, které jsou nezbytné pro použití této příručky a také se odkázat na normu ISO/IEC 27001:2005.

3. Termíny a definice

Obsah této kapitoly odpovídá kapitole 4.1 této práce. Jde o vysvětlení základních pojmů z oblasti ISMS. Dále je vhodné pojmy z kapitoly 4.1 dle normy rozšířit o: Bezpečnostní incident, zbytkové riziko, přijetí rizika, analýza rizik, míra rizika, zvládání rizik, snižování rizik a prohlášení o aplikovatelnosti.

4. Systém managementu bezpečnosti informací

Jde o stěžejní a nejrozsáhlejší kapitolu příručky bezpečnosti informací. V této části je popsán celý proces ISMS a odpovídá tak kapitole 4.5 o postupu zavádění ISMS. Popisuje se fáze *ustavení ISMS* což obnáší definování **rozsahu a hranic** ISMS. Rozsah platnosti je určen dislokačně, provozní budovou firmy a seznamem aktiv zahrnutých do procesu ISMS. Zde je možno použít seznam aktiv z kapitoly 6.1.1. A dále předmětem podnikání.

Druhou podkapitolou je **politika ISMS.** Zde je vhodné se odkázat na vypracovaný dokument politiky ISMS. V něm vedení vyjadřuje podporu bezpečnosti informací v podniku a definuje klíčové zásady bezpečnosti.

Třetí podkapitolou je **přístup organizace k hodnocení rizik**. Zde je popsán způsob hodnocení aktiv, hrozeb a výpočtu rizika tak, jak uvádí kapitola 4.6 popisující teorii analýzy rizik a také kapitola 6.1 zabývající se konkrétní aplikací vybrané metody.

Následuje matice rizik a jejich zhodnocení. Další kapitoly se pak věnují zavádění jednotlivých **bezpečnostních opatření** tak, jak je popsáno v kapitole 6.2 této práce. Jde o nejrozsáhlejší část příručky. Následuje odkaz na **prohlášení o aplikovatelnosti** a **přijetí zbytkových rizik** vedením.

Další fází je *zavádění a provoz ISMS*. Ta obnáší formulaci **plánu zvládání rizik** a **prohlubování bezpečnostního povědomí zaměstnanců**. Zde by měly být rozebrány všechny programy plánovaných školení zaměstnanců a další způsoby zajištění požadované kvalifikace, včetně zaměstnání kvalifikovaného personálu. Cílem tohoto postupu je vytvoření potřebného povědomí personálu o závažnosti a významu svých činností v rámci bezpečnosti informací.

Následuje *Monitorování a přezkoumání ISMS.* Tato fáze popisuje monitorování procesu ISMS a přezkoumání jeho účinnosti. Výsledky těchto zjištění jsou podnětem pro přehodnocení výsledků hodnocení rizik.

Udržování a zlepšování ISMS – zde jsou rozvedena opatření k nápravě a preventivní opatření.

5. Odpovědnost vedení

Zde by měl být jmenován tým pro implementaci a provoz ISMS. Dále by neměl chybět závazek vedení vůči ISMS, ve kterém vedení projevuje vůli k ustavení, zavedení, provozu, monitorování, přezkoumání, udržování a zlepšování ISMS, a také definuje jakými prostředky je toho docíleno včetně poskytování dostatečných finančních zdrojů, prohlubování bezpečnostního povědomí zaměstnanců a soustavného zlepšování celého procesu na základě interních auditů.

6. Interní audity ISMS

Organizace provádí interní audity ISMS v plánovaných intervalech pro ověření, že politika a cíle bezpečnosti informací, jakož i jednotlivá bezpečnostní opatření a procesy spojené s ISMS:

- Vyhovují požadavkům této normy a odpovídajícím zákonným požadavkům.
- Vyhovují identifikovaným požadavkům na bezpečnost informací.
- Jsou zavedeny a udržovány efektivně.
- Fungují tak, jak se očekává.

7. Přezkoumání ISMS vedením organizace

Vedení organizace provádí přezkoumání ISMS organizace v intervalu min jednou za rok pro zajištění jeho neustálé aktuálnosti a účinnosti.

Tato přezkoumání hodnotí možnosti:

- Zlepšení.
- Potřebu změn v ISMS, včetně bezpečnostní politiky a cílů bezpečnosti.

Výsledky přezkoumání jsou jasně zdokumentovány ve zprávě Přezkoumání ISMS a jsou o nich vedeny záznamy.

Vstupy pro přezkoumání vedením organizace zahrnují informace o:

- Výsledcích auditů.
- Zpětné vazbě od zainteresovaných stran.
- Technikách a postupech, které by mohly být použity pro zlepšení účinnosti ISMS.
- Stavu preventivních opatření a stavu opatření k nápravě.
- Zranitelnostech a hrozbách, jimž dosud nebyla věnována náležitá pozornost.
- Závěrech měření účinnosti zavedených opatření.
- Činnostech, které následovaly po předchozím přezkoumání vedením organizace.
- Změnách, které by mohly ovlivnit ISMS.
- Doporučeních pro zlepšení.

Výstup z přezkoumání prováděného vedením organizace zahrnuje rozhodnutí a činnosti vztahující se k:

- Zvyšování účinnosti ISMS.
- Aktualizaci hodnocení rizik a plánu zvládání rizik.
- Nezbytným změnám postupům, které se mohou týkat:
    - Požadavků spojených s činností organizace.
    - Bezpečnostních požadavků.
    - Smluvních závazků.
    - Regulatorních nebo zákonných požadavků.
    - Úrovní rizika anebo úrovní akceptovatelnosti rizika.

8. Zlepšování ISMS

Poslední kapitola příručky popisuje zavedený a dokumentovaný postup neustálého zlepšování a zvyšování účinnosti ISMS.

Pro identifikaci příležitostí ke zlepšení jsou využity:

- Politika bezpečnosti informací.
- Cíle bezpečnosti informací.
- Výsledky auditů.
- Analýzy monitorovaných událostí.
- Nápravná a preventivní opatření.
- Přezkoumání ISMS prováděných vedením organizace.

Organizace průběžně identifikuje změny rizik, čímž vznikají požadavky na opatření k nápravě, zejména pak u těch rizik, jejichž změna byla významná. Priorita opatření k nápravě je určena na základě výsledků hodnocení rizik.

Jsou také definovány požadavky na identifikaci potenciálních nesouladů a jejich příčin, určení a zavedení potřebných preventivních opatření, přezkoumání provedených preventivních opatření a zaznamenání výsledků podniknutých opatření.

7 Závěr

Cílem této diplomové práce bylo navrhnout postup pro zavedení managementu bezpečnosti informací ve zvoleném podniku a dále vypracovat metodiku pro návrh podoby příručky ISMS.

Postup byl takový, že v teoretické části byly nejprve popsány základní pojmy a procesy používané v oblasti bezpečnosti informačních systémů. Poté byl vytvořen přehled norem a zákonů, použitelných při implementaci ISMS. Konkrétně byla rozebrána rodina norem řady ČSN ISO/IEC 27000. V další části teorie je popsán všeobecný postup zavádění ISMS v organizaci metodou systémového přístupu.

Následovala stěžejní část celého procesu, tedy řízení rizik a důkladný popis obecných postupů a používaných metod. Tato teoretická část tvoří shrnutí pro management podniku a slouží k rychlému pochopení, jaký je princip zavádění ISMS v podniku.

Další část práce obsahuje důkladnou analýzu aktuálního stavu bezpečnosti informací ve vybraném podniku. Pro lepší zmapování reálného stavu byl vytvořen a rozeslán anonymní dotazník zaměstnancům firmy. Z jeho výsledků vyplynuly zajímavé skutečnosti ohledně bezpečnostního povědomí pracovníků a úrovně bezpečnosti informací v podniku.

V praktické části je na základě teoretických předpokladů navrhnuta a popsána metodika zpracování analýzy rizik informací konkrétní organizace. Analýza rizik byla řešena pomocí kvalitativních metod, které umožňují poměrně snadno a rychle identifikovat riziko v určitém rozsahu. V prvním kroku se identifikovala aktiva spolu s hrozbami a provedlo se jejich ohodnocení. Dále byla sestavena matice zranitelností a matice rizik pro vyjádření úrovní jednotlivých rizik. Na základě analýzy rizik byla vybrána vhodná opatření, která mají za úkol tato rizika snižovat a chránit tak identifikovaná aktiva.

Vzhledem k velikosti podniku a charakteru podnikatelské činnosti jsem při návrhu opatření vycházel z personálních, časových a finančních možností dané organizace, a následně těmto podmínkám přizpůsobil i plán postupného zavádění opatření.

Posledním úkolem bylo navrhnout podobu a strukturu příručky bezpečnosti informací pro tento podnik. Cíle práce byly tedy splněny.

Praktické zavedení jednotlivých opatření do každodenního provozu fungující organizace vždy přináší určité restrikce vůči zaměstnancům a klade na ně požadavky, na něž dosud nebyli zvyklí. Zatímco restriktivní složka těchto opatření je patrná hned a pracovník ji pocítí s okamžitě, přínos daných opatření už tak snadno a jasně vidět není a obvykle se projeví až po určitém časovém úseku. Je v lidské přirozenosti, se změnám (pro ně subjektivně k horšímu) bránit, proto je prosazení nových opatření a zavádění nových struktur velmi nesnadný úkol. (16)

7.1 Ekonomické zhodnocení projektu

V této podkapitole bych rád shrnul a vyzdvihnul ekonomické přínosy navrhovaných bezpečnostních opatření. Jak již bylo vyčísleno v kapitole 6.2.11 (Ekonomická rozvaha projektu), celkové náklady na zavedení vybraných opatření z kapitoly 6.2, včetně provedení bezpečnostního testu, jsou 525 000 Kč. Jde o náklady na zavedení a jeden rok provozu systému ISMS. V návaznosti na tato nová opatření byla přepracována analýza rizik s upravenými pravděpodobnostmi některých hrozeb a zranitelností. Výsledek přepracované matice rizik je součástí přílohy 3. Porovnání počtu rizik je uvedeno v Tabulka 7.

počet rizik	Před zavedením	Po zavedení
Vysokých	5	0
Středních	81	19
Nízkých	276	262

Tabulka 7: porovnání rizik před a po zavedení opatření

Z tohoto porovnání je patrné, že navrhovaná opatření úplně eliminovala vysoká rizika podniku, která jsou nepřípustná. Byla odstraněna i většina středních rizik, ale odstranění všech by si vyžádalo neúměrně vysoké náklady, proto bylo rozhodnuto o jejich retenci. Mezi nízká rizika se přesunula snížená rizika z předchozích kategorií, přičemž některá byla taktéž eliminována.

Posouzení ekonomické výhody zavedených opatření je možno provést na základě vyčíslení škod, ke kterým by mohlo dojít v případě, že by opatření přijata nebyla. Jako vhodný příklad se jeví jakákoliv porucha vybavení serverovny a následný výpadek informačního systému. Jelikož je výroba ve firmě plně řízena tímto systémem a veškeré

operace s polotovary a materiály jsou přes čtečky čárových kódů propojeny se systémem, dochází pří výpadku k úplnému zastavení výroby.

Na základě konzultace s vedením firmy byla odhadnuta denní produkce firmy na 350 kusů výrobků, přičemž cena materiálu je průměrně 500 Kč na kus a prodejní cena 1 000 Kč. Podniku tedy při výpadku výroby vznikne denně škoda 175 000 Kč, ve které jsou zahrnuty výrobní režie, platy a ušlý zisk. Výhodnost zavedení ISMS lze prokázat tedy velice snadno. Stačí k tomu jednoduchý příklad závady ventilátoru na 4 roky starém serveru, který je trvale v provozu a neexistuje závazný plán údržby a čištění. Navíc je umístěn v malém a plně obsazeném racku. Tato drobná závada způsobí přehřátí a poruchu serveru, čímž se zastavuje chod firmy. Během prvního dne je zjištěn problém a rychle se shání náhradní server. Objednávka nového serveru by však trvala více než týden, je proto zajištěno náhradní řešení a druhý den je server namontován a zapojen. Během třetího dne je na něm zprovozněn informační a výrobní systém, výroba může opět pokračovat. Při tomto drobném incidentu, kdy dokonce nebyla ztracena žádná data, však vznikla vyšší škoda, než kolik by stálo zavedení a roční provoz ISMS s opatřeními, které mimo jiné zahrnují úplně nový, spolehlivý server s pětiletou zárukou okamžité dodávky náhradního, a také zavádí plány pravidelné údržby zařízení, které by těmto problémům mohly zabránit.

Druhý příklad ekonomického přínosu je výrazný výkonový rozdíl nového serveru a tedy lepší dostupnost služeb IS a rychlejší odezva. Každý den je potřeba před zahájením výroby provést její plán. To je náročná operace pro výrobní systém propojený s informačním systémem a operující nad firemní databází. Na stávajícím serveru tato operace často trvá i více než hodinu a vedoucí pracovníci výroby do té doby nemohou výrobu zahájit. Na novém serveru, který má místo 4GB paměti 24GB a několikrát výkonnější procesor, by daný úkol trval pouze v řádech minut.

I kdyby přínosy opatření nebyly v praxi tak účinné, jak vyplynulo z analýzy rizik, firmě se tato investice do ISMS rozhodně vyplatí.

8 Použitá literatura

(1) ČSN ISO/IEC 27001:2006. Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2006.

(2) ČSN ISO/IEC 27002:2006. Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. ČNI 2008.

(3) ČSN ISO/IEC 27005:2009. Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informaci. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009.

(4) Zákon č. 101/2000 Sb., o ochraně osobních údajů [online]. 2000 [cit. 2013-05-02]. Dostupné na URL: <http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&loc=20>.

(5) ADÁSKOVÁ, P. Systematický přístup k výběru vhodné metody analýzy rizik v organizaci [online]. 2008 [cit. 2013-05-02]. Dostupné na URL: <http://www.risk-management.cz/index.php/tisk.php?clanek=3727>.

(6) ČERMÁK, M., Řízení informačních rizik v praxi. 1. vyd. Brno: Tribun EU, 2009. 134s. ISBN 978-80-7399-731-1.

(7) DOUCEK, P. NOVÁK, L., SVATÁ, V. Řízení bezpečnosti informací. 1. vyd. Příbram: Professional publishing 2008. 239s. ISBN 978-80-86946-88-7.

(8) GOGELA, R. Standardy a definice pojmů bezpečnosti informací 2011. ISBN 978-80-7251-356-7 [online]. [cit. 2013-03-28]. Dostupné na URL: <http://www.cybersecurity.cz/data/Gogela.pdf>.

(9) NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti. CyberSecurity.cz - Kybernetická bezpečnost [online]. [cit. 2013-04-16]. Dostupné na URL: <www.cybersecurity.cz/data/SRIB.pdf>.

(10) POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. 2005. 309 s. ISBN 80-86898-38-5.

(11) SMEJKAL, V., RAIS, K., Řízení rizik ve firmách a jiných organizacích, 3. Vyd. Grada Publishing, Praha, 2010, ISBN 978-80-247-3051-6.

(12) ŠUSTR, Josef. Politika informační bezpečnosti organizace. In: Systemonline.cz [online]. 2001 [cit. 2013-04-07]. Dostupné na URL: <http://www.systemonline.cz/clanky/politika-informacni-bezpecnosti-organizace.htm>.

(13) ISMS - Seriál o řízení bezpečnosti [online]. [cit. 2013-04-02]. Dostupné na URL: <http://www.chrantesidata.cz/cs/art/472/>.

(14) Prezentace služeb firmy Agerit s.r.o. [online]. [cit. 2013-05-12]. Dostupné na URL: <http://test.bezpecnosti.cz/sluzby_ceny.php>.

(15) Slovník zkratek [online]. [cit. 2013-04-26]. Dostupné na URL: <http://www.zkratky.cz>.

(16) Jak vypracovat bezpečnostní politiku organizace [online]. [cit. 2013-05-12]. Dostupné na URL: <http://computerworld.cz/securityworld/jak-vypracovat-bezpecnostni-politiku-v-podniku-46442>.

Seznam příloh

Informační bezpečnost středně velkého podniku

Anonymní dotazník určený managementu, administrativním a vývojovým pracovníkům, zaměřený na povědomí o bezpečnosti při nakládání s informacemi.
*Povinné pole

Stalo se Vám, že jste přišli o svá data? *
např. selháním hardwaru/softwaru, omylem, cizím zaviněním

- ( ) Ano
- ( ) Ne

Chráníte svůj počítač heslem? *
pro přihlášení do Windows

- ( ) Ano
- ( ) Ne

Uchováváte ve svém počítači pro firmu důležitá data? *
data, která jsou pouze ve vašem počítači a nejsou kopírována do firemního informačního systému, příp. na datový server

- ( ) Ano
- ( ) Ne
- ( ) Nevím

Došlo někdy k modifikaci vašich dat jiným člověkem bez vašeho vědomí? *
smazání / modifikace vašich dat v informačním systému / na serveru. Zásah IT technika do vašeho počítače

- ( ) Ano
- ( ) Ne
- ( ) Nevím

Jakým způsobem probíhá výměna dat mezi pracovníky uvnitř podniku? *
zatrhněnte všechny možnosti, které využíváte

- [ ] firemní email
- [ ] soukromý email
- [ ] v papírové podobě
- [ ] flash disk (firemní)
- [ ] flash disk (soukromý)
- [ ] firemní datový server
- [ ] firemní informační systém
- [ ] Jiné:

Pokuste se odhadnout jakou hodnotu má pro vaši firmu hardwarové vybavení *
počítače, servery, tiskárny, síťová infrastruktura

	1	2	3	4	5	
relativně nízká	( )	( )	( )	( )	( )	relativně vysoká

Pokuste se odhadnout jakou hodnotu má pro vaši firmu softwarové vybavení *
operační systémy, programy, podnikový informační systém

	1	2	3	4	5	
relativně nízká	( )	( )	( )	( )	( )	relativně vysoká

Pokuste se odhadnout jakou hodnotu mají pro vaši firmu data uložená ve firmě *
schémata, dokumentace, databáze, výrobní postupy, obchodní údaje

	1	2	3	4	5	
relativně nízká	◯	◯	◯	◯	◯	relativně vysoká

Je ve vaší firmě nějakým způsobem upravena politika bezpečnosti firemních informací a pravidla pro chování v podnikové síti? *
dokument / příručka / směrnice

- ◯ Ano
- ◯ Ne
- ◯ Nevím

Účastnili jste se někdy bezpečnostního školení v této oblasti? *
(bezepečnost práce s informacemi, informačním systémem, chování v síti atd.)

- ◯ Ano
- ◯ Ne

Zálohujete pravidelně data ve vašem počítači? *
data, která nejsou uložena v informačním systému / datovém serveru a fyzicky se nacházejí pouze na vašem počítači

- ◯ Ano
- ◯ Někdy
- ◯ Nikdy
- ◯ Zálohování má na starosti správce IT
- ◯ Vše důležité ukládám na server / do informačního systému

Vyžaduje povaha vaší práce přístup do firemního informačního systému? *
během pracovní doby

- ◯ Ano, ale přístup tam nemám
- ◯ Ano, přístup mám
- ◯ Ne, ale přístup tam mám
- ◯ Ne, přístup nemám

Vyžaduje povaha vaší práce přístup k internetu? *

- ◯ Ano, ale přístup k němu nemám
- ◯ Ano, přístup mám
- ◯ Ne, ale přístup k němu mám
- ◯ Ne, přístup nemám

Monitoruje váš zaměstnavatel nějakým způsobem vaši aktivitu na internetu? *
během pracovní doby

- ◯ Ano
- ◯ Ne
- ◯ Nevím

Omezuje váš zaměstnavatel nějakým způsobem možnost instalace nových programů do pracovního počítače? *
např. omezením plného přístupu k systému

- ◯ Ano, v případě potřeby je nutné kontaktovat správce IT
- ◯ Neomezuje, mohu instalovat jakékoliv programy, které potřebuji
- ◯ Nevím, dosud nebylo potřeba nic instalovat

Jak hodnotíte úroveň zabezpečení firemních dat uvnitř firmy? *
z hlediska zaměstnance, který by chtěl zneužít/poškodit firemní data

1 2 3 4 5

slabé zabezpečení ◯ ◯ ◯ ◯ ◯ silné zabezpečení

Jak hodnotíte úroveň vnějšího zabezpečení firemních dat? *
z hlediska externího narušitele, který by chtěl získat/zničit firemní data

1 2 3 4 5

slabé zabezpečení ◯ ◯ ◯ ◯ ◯ silné zabezpečení

S jakými z těchto bezpečnostních incidentů jste se ve firmě již setkali? *
zatrhněte všechny možnosti

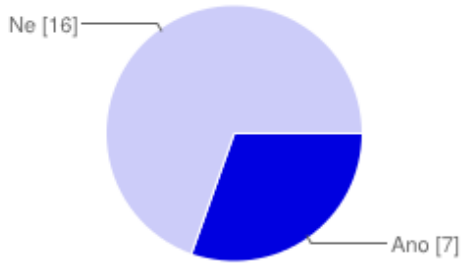
- ☐ Výpadek el. proudu
- ☐ Nedostupnost firemní sítě
- ☐ Selhání hardwaru počítače
- ☐ Počítačový virus
- ☐ Zahlcení SPAMem
- ☐ Krádež zařízení
- ☐ Chyba uživatele / administrátora
- ☐ Jiné:

Poznámky k úrovni bezpečnosti informací v podniku i k samotnému dotazníku
Nepovinné

Odeslat

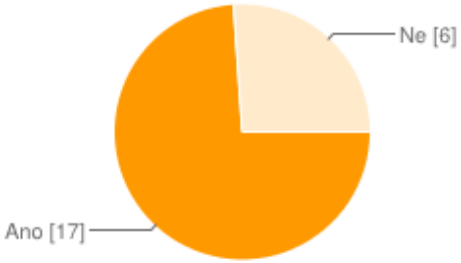
Nikdy přes Formuláře Google neposílejte hesla.

Stalo se Vám, že jste přišli o svá data?



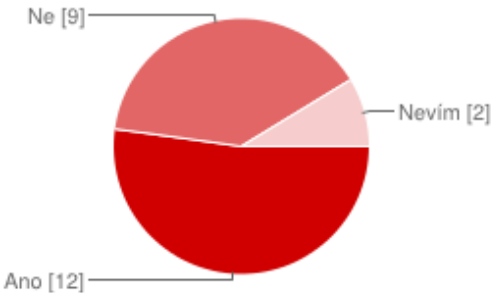
Ano	**7**	30%
Ne	**16**	70%

Chráníte svůj počítač heslem?



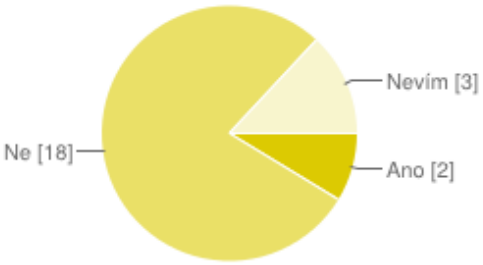
Ano	**17**	74%
Ne	**6**	26%

Uchováváte ve svém počítači pro firmu důležitá data?



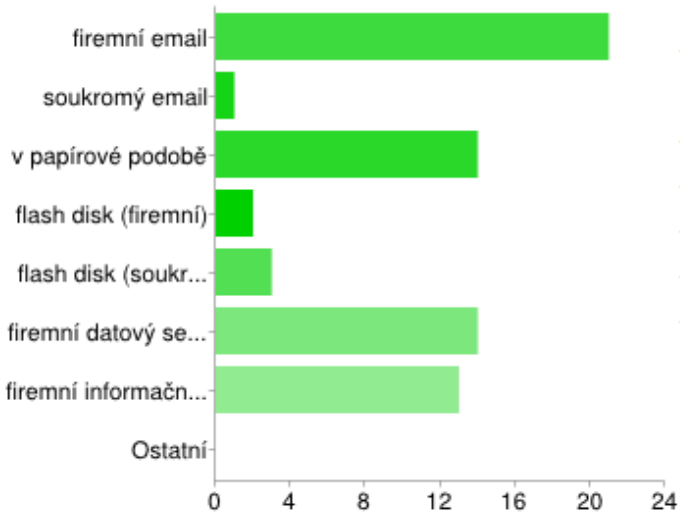
Ano	**12**	52%
Ne	**9**	39%
Nevím	**2**	9%

Došlo někdy k modifikaci vašich dat jiným člověkem bez vašeho vědomí?



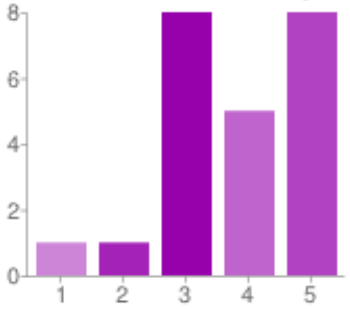
Ano	**2**	9%
Ne	**18**	78%
Nevím	**3**	13%

Jakým způsobem probíhá výměna dat mezi pracovníky uvnitř podniku?



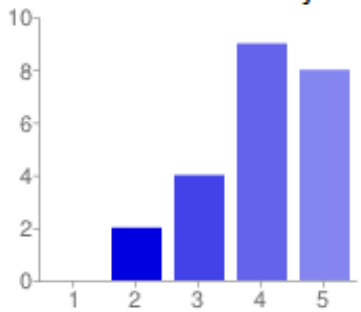
firemní email	**21**	31%
soukromý email	**1**	1%
v papírové podobě	**14**	21%
flash disk (firemní)	**2**	3%
flash disk (soukromý)	**3**	4%
firemní datový server	**14**	21%
firemní informační systém	**13**	19%
Ostatní	**0**	0%

Pokuste se odhadnout jakou hodnotu má pro vaši firmu hardwarové vybavení



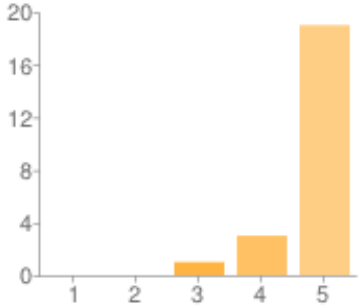
1	**1**	4%
2	**1**	4%
3	**8**	35%
4	**5**	22%
5	**8**	35%

Pokuste se odhadnout jakou hodnotu má pro vaši firmu softwarové vybavení



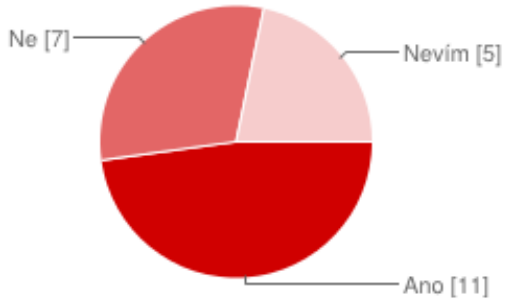
1	**0**	0%
2	**2**	9%
3	**4**	17%
4	**9**	39%
5	**8**	35%

Pokuste se odhadnout jakou hodnotu mají pro vaši firmu data uložená ve firmě



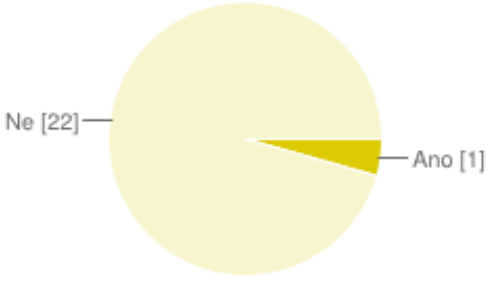
1	**0**	0%
2	**0**	0%
3	**1**	4%
4	**3**	13%
5	**19**	83%

Je ve vaší firmě nějakým způsobem upravena politika bezpečnosti firemních informací a pravidla pro chování v podnikové síti?



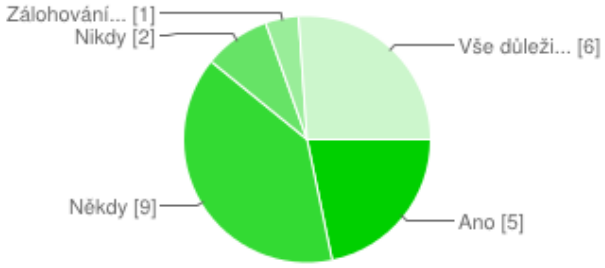
Ano	**11**	48%
Ne	**7**	30%
Nevím	**5**	22%

Účastnili jste se někdy bezpečnostního školení v této oblasti?



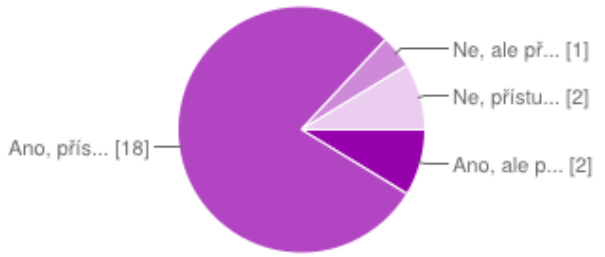
Ano	**1**	4%
Ne	**22**	96%

Zálohujete pravidelně data ve vašem počítači?



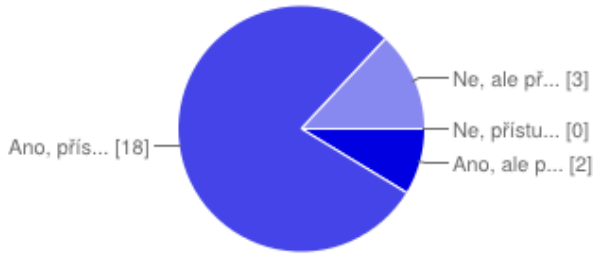
Ano	5	22%
Někdy	9	39%
Nikdy	2	9%
Zálohování má na starosti správce IT	1	4%
Vše důležité ukládám na server / do informačního systému	6	26%

Vyžaduje povaha vaší práce přístup do firemního informačního systému?



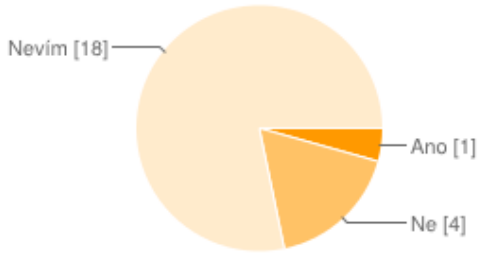
Ano, ale přístup tam nemám	2	9%
Ano, přístup mám	18	78%
Ne, ale přístup tam mám	1	4%
Ne, přístup nemám	2	9%

Vyžaduje povaha vaší práce přístup k internetu?



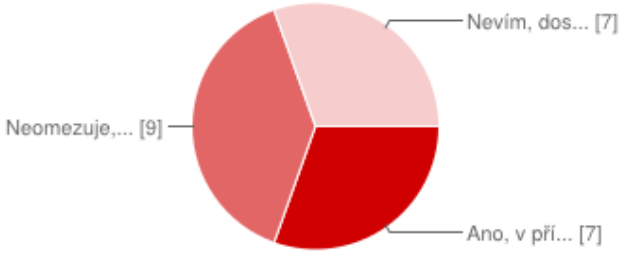
Ano, ale přístup k němu nemám	2	9%
Ano, přístup mám	18	78%
Ne, ale přístup k němu mám	3	13%
Ne, přístup nemám	0	0%

Monitoruje váš zaměstnavatel nějakým způsobem vaši aktivitu na internetu?



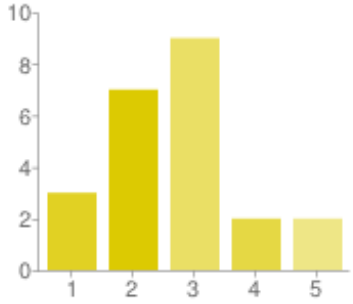
Ano	1	4%
Ne	4	17%
Nevím	18	78%

Omezuje váš zaměstnavatel nějakým způsobem možnost instalace nových programů do pracovního počítače?



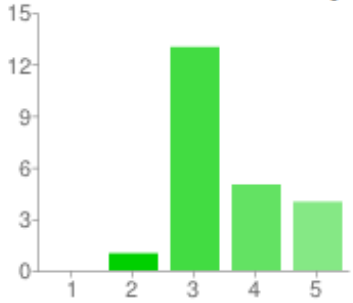
Ano, v případě potřeby je nutné kontaktovat správce IT	7	30%
Neomezuje, mohu instalovat jakékoliv programy	9	39%
Nevím, dosud nebylo potřeba nic instalovat	7	30%

Jak hodnotíte úroveň zabezpečení firemních dat uvnitř firmy?



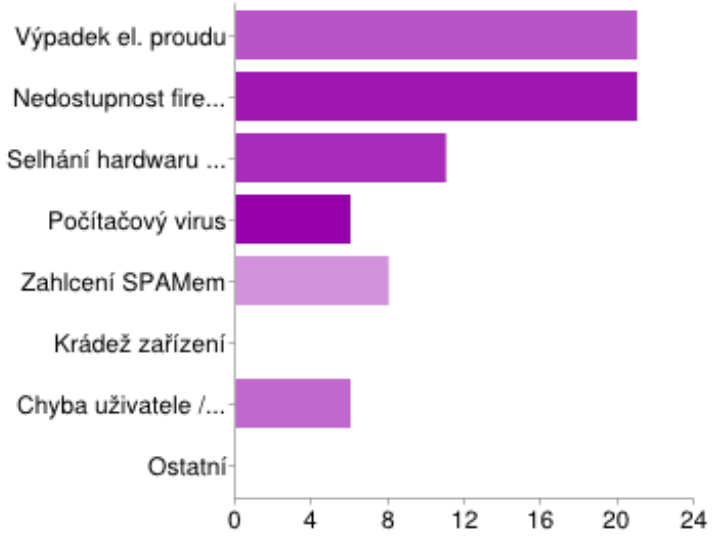
1	**3**	13%
2	**7**	30%
3	**9**	39%
4	**2**	9%
5	**2**	9%

Jak hodnotíte úroveň vnějšího zabezpečení firemních dat?



1	**0**	0%
2	**1**	4%
3	**13**	57%
4	**5**	22%
5	**4**	17%

S jakými z těchto bezpečnostních incidentů jste se ve firmě již setkali?



Výpadek el. proudu	**21**	29%
Nedostupnost firemní sítě	**21**	29%
Selhání hardwaru počítače	**11**	15%
Počítačový virus	**6**	8%
Zahlcení SPAMem	**8**	11%
Krádež zařízení	**0**	0%
Chyba uživatele / administrátora	**6**	8%
Ostatní	**0**	0%

		Poškození vodou	Poškození bleskem	Poškození požárem	Výpadek el. proudu	Výpadek internetu	Poškození prachem	Krádež zařízení	Krádež dokumentů/médií	Vnější útok	Interní sabotáž	Počítačový virus	Pomsta býv. zaměstnance	Nedodržení směrnic a postupů	Podvržená uživ. identita	Porušení mlčenlivosti zam.	Neop. získání přís. práv	Zneužití přístup. oprávnění	Selhání HW	Selhání SW	Selhání sítě	Nedost. bezp. povědomí zam.	Por. vzduchotech. serverovny	Únik důvěrných informací	Chyba uživatele ICT	
		1	3	1	3	3	4	3	3	2	2	3	2	3	3	3	3	3	3	3	4	4	2	2	5	max
Server Linux	4	0	12	4	12	36	16	12	0	16	8	0	0	12	0	0	0	0	12	0	0	32	16	0	40	40
Server Windows	4	0	12	4	12	0	16	12	0	0	8	0	0	12	0	0	0	0	12	0	0	32	16	0	40	40
HDD serveru	5	0	15	5	15	0	20	15	0	0	20	0	0	15	0	0	0	0	15	0	0	60	20	0	0	60
Router	2	0	6	2	0	0	0	0	0	8	4	0	0	0	0	0	0	0	6	0	24	0	0	0	20	24
Modem	2	0	6	2	0	0	0	0	0	0	4	0	0	0	0	0	0	0	6	0	24	0	0	0	0	24
UPS zdroj	3	0	9	3	0	0	0	0	0	0	6	0	0	0	0	0	0	0	9	0	0	0	0	0	0	9
Switche	3	0	9	3	0	0	0	0	0	0	6	0	0	0	0	0	0	0	9	0	36	0	0	0	15	36
Kamerový systém	1	3	9	2	9	6	8	0	0	6	4	0	4	0	0	0	0	0	9	0	0	8	0	0	0	9
Video server	1	0	3	1	0	0	0	0	0	0	2	0	0	0	0	0	0	0	3	0	0	0	0	0	0	3
Tiskárny	1	1	6	2	9	0	4	3	0	0	4	0	0	0	0	0	0	0	3	0	0	0	0	0	0	9
Pracovní stanice zaměstnanců	2	4	12	4	12	0	8	0	0	4	8	0	0	6	0	0	0	0	6	0	0	8	0	0	20	20
HDD pracovních stanic	3	9	18	6	18	0	12	0	0	6	18	0	0	9	0	0	0	0	18	0	0	24	0	0	0	24
Podniková síť	3	6	18	9	18	18	0	0	0	0	12	0	0	9	0	0	0	0	18	0	0	24	0	0	30	30
Dataprojektor	1	1	3	1	6	0	8	6	0	0	2	0	0	0	0	0	0	0	3	0	0	0	0	0	0	8
MS Windows Server 2003	4	0	0	0	0	0	0	0	0	0	0	24	0	24	24	0	24	24	0	36	0	16	0	0	20	36
Linux Debian	4	0	0	0	0	0	0	0	0	0	0	36	0	24	24	0	24	24	0	36	0	16	0	0	40	40
SAP Business One ERP	5	0	0	0	0	0	0	0	0	0	0	0	0	30	45	0	75	30	0	30	0	40	0	0	75	75
MS SQL databáze	4	0	0	0	0	0	0	0	0	0	0	24	0	24	24	0	24	24	0	36	0	16	0	0	60	60
Operační systémy prac. stanic	3	0	0	0	0	0	0	0	0	0	0	27	0	9	9	0	9	9	0	27	0	12	0	0	30	30
Codewarrior	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	10	10
Autocad	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	20	20
Docházkový systém	3	0	0	0	0	0	0	0	0	0	0	0	18	9	18	0	18	9	0	27	0	12	0	0	45	45
Účetní program	2	0	0	0	0	0	0	0	0	0	0	12	0	6	0	0	0	0	0	18	0	0	0	0	30	30
Výrobní IS	4	0	0	0	0	0	0	0	0	0	0	0	0	24	24	0	24	12	0	36	0	16	0	0	60	60
MS Office	2	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	12	0	0	0	0	10	12
Projekty a plány	5	0	0	5	0	0	0	0	15	0	20	0	0	30	45	15	60	30	0	0	0	20	0	30	50	60
Zálohy dat	5	0	0	10	15	0	0	30	30	0	20	15	0	45	45	0	45	15	0	0	40	60	0	0	50	60
Rozpracované dokumenty na pc	3	0	0	3	9	0	0	0	9	0	12	18	0	18	27	9	27	9	0	0	0	24	0	6	30	30
Zdrojové kódy programů	4	0	0	4	12	0	0	0	12	0	24	12	0	36	0	12	0	0	0	0	0	32	0	24	40	40
Osobní údaje zaměstnanců	5	0	0	0	0	0	0	0	15	0	30	30	0	45	0	15	0	0	0	0	0	40	0	30	50	50
Účetnictví	4	4	0	8	0	0	0	0	12	0	8	0	0	36	0	12	0	0	0	0	0	0	0	8	0	36
Smlouvy s dodavateli/odběrateli	3	3	0	6	0	0	0	0	9	0	6	0	0	18	0	9	0	0	0	0	0	12	0	6	0	18
Výrobní dokumentace	5	5	0	10	0	0	0	0	15	0	10	0	0	45	0	15	0	0	0	0	0	20	0	10	0	45
Licenční smlouvy	3	3	0	6	0	0	0	0	9	0	6	0	0	18	0	0	0	0	0	0	0	12	0	0	0	18
Dokumentace projektů	4	4	0	8	0	0	0	0	12	0	8	0	0	36	0	24	0	0	0	0	0	16	0	24	0	36
Připojení k Internetu	2	0	0	0	0	0	0	0	0	8	0	12	0	0	0	0	0	0	12	0	0	0	0	0	0	12
Web společnosti	1	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	9	9	0	0	0	0	0	0	0	9
Elektronická pošta	3	0	0	0	0	0	0	0	0	6	6	18	12	27	0	0	0	0	0	18	48	24	0	0	30	48
Budova	4	12	12	16	0	0	0	0	0	0	8	0	16	0	0	0	0	0	0	0	0	0	0	0	0	16
	max	12	18	16	18	36	20	30	30	16	30	36	18	45	45	24	75	30	18	36	48	60	20	30	75	

Přepočítaná matice rizik po zavedení navrhnutých bezpečnostních opatření